Gainsborough Adventure Playground Ltd

Data Protection Policy

Introduction

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

Types of Data Held
We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into an application form or included in a cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:

    i) job title and job descriptions
    ii) your salary
    iii) your wider terms and conditions of employment
    iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    v) internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

Employee Rights
You have the following rights in relation to the personal data we hold on you:

h) the right to be informed about the data we hold on you and what we do with it;
i) the right of access to the data we hold on you. More information on this can be found in the section headed “Access to Data” below and in our separate policy on “Subject Access Requests”;
j) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as ‘rectification’;
k) the right to have data deleted in certain circumstances. This is also known as ‘erasure’;
l) the right to restrict the processing of the data;
m) the right to transfer the data we hold on you to another party. This is also known as ‘portability’;
n) the right to object to the inclusion of any information;
o) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

Responsibilities
In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

Lawful Bases of Processing
We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

Access to Data
As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

Data Disclosures
The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

p) any employee benefits operated by third parties;
q) disabled individuals - whether any reasonable adjustments are required to assist them at work;
r) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
s) for Statutory Sick Pay purposes;
t) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
u) the smooth operation of any employee insurance policies or pension plans;
v) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security
All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Third Party Processing
Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

International Data Transfers
The Company does not transfer personal data to any recipients outside of the EEA.

Requirement to Notify Breaches
All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

Training
New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Records
The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

Data Protection Compliance

Our Data Protection Officers are:
Lisa Pinkney and Claire Jones

Registered Children Rights
To ensure that where information is stored, or processed steps are taken to ensure that this information is stored or processed in accordance with the Data Protection Act 1998. GAPA is committed to keeping personal information about children and families as secure as possible.

It is the responsibility of all members of staff to ensure that the personal information about children and families is not shared with individuals outside the setting, The Company Manager has overall responsibility to ensure that all personal information is kept safe and secure and in compliance with the Data Protection Act 1998.

ALL PARENTS/CARES/GUARDIANS SHOULD BE MADE AWARE THAT IN THE EVENT OF A CHILD PROTECTION CONCERN THEN INFORMATION ABOUT THEIR FAMILIES MAY BE SHARED WITH THE RELEVANT AGENCIES WITHOUT THEIR CONSENT

How Is Children and Families Personal Information Stored At GAPA

Personal information including:

- Children's details such as name address, dates of birth, school, ethnicity, additional needs, medical needs, allergies
- Parents information such as name and address, telephone numbers

We have a section on the registration form of optional questions which parents can choose if they want to share or not. The replies are purely for monitoring purposes and are only shared with other agencies as part of collated statistics and are totally anonymous.

Other information including:

- Accident records
- Incident record's
- Administration of Medicine records

May be stored in 2 forms:

1) Paper: paper copies of personal information are stored in a locked cabinet which has limited access to staff members and no access for parents. Parents should feel secure that their information and information about their child is not accessible to anyone apart from themselves and GAPA staff
2) Computer: any information that is stored on computer will be held in accordance with the Data Protection Act 1998. Parents will be asked for their permission to store their personal details on computer when registering their children. Access to information stored on computer is limited to staff members, all GAPA computers are password protected and only management are in possession of the Company Managers password. If any parent would like access to their information stored on computer, then they must be accompanied by a member of staff who will display only the requisite information and will remain in the room with the parent to ensure data protection for all other families.

All individual, parents, carer's & guardians have the right of access to manual and computerised records when concerning their personal data. Where it is deemed necessary to divulge a third party this will only be done with the express permission of the individual subject. Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be hard copy (paper) format and computer files.

Outings
When taking children on outings the group leader will hold all the emergency and contact forms in case parents/cares need to be contacted whilst on the trip or medical assistance is needed, at the end of the trip the forms will be shredded immediately.

Data in Transit
We do not encourage staff to take home mobile devices such as laptops home but if the need arises then the following needs to be adhered to:

- They never leave it in the car or on any form of transport
- They keep it locked securely when not using the device
- They do not let anyone use or see documents
- If anyone is over the age of 16 years in the house they ensure again it locked away securely
- Computer passwords are used not shared and fire walls and security are kept up to date on the device
- If it gets lost or stolen they must report it immediately to Manager or Owner
- The device is password protected