DATA PROTECTION POLICY

Approved by: Régine Natchoo Date: 25 May 2018

Last reviewed on: 25 May 2018

Next review due by: 25 May 2019

1. Aims

Funtastic Club aims to ensure that all personal data collected about staff, children, parents, visitors and other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)** and the expected provisions of the Data Protect Act 2018 (DPA2018) as set out in the **Data Protection Bill**.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the **GDPR** and the ICO's **code of practice for subject access requests**.

3. Definitions

Personal data:
Any information relating to an identified, or identifiable, individual.
This may include the individual's:
Full name
Identification
Location data
Email address
It may also include factors specific to the individual's physical, physiologic, genetic, mental, economic, cultural or social identity.

Special categories of persona data:
Personal data which is more sensitive and so needs more protection, including information about an individual's:
Racial or Ethnic origin
Religious or philosophical beliefs
Genetics
Health – physical or mental
Criminal convictions
Disabilities

Processing:
Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

Data subject:
The identified or identifiable individual whose personal data is held or processed.

Data controller:
A person or organisation that determines the purposes and the means of processing of personal data.

Data processor:
A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Funtastic Club processes personal data relating to parents, children, staff, visitors and others, and therefore is a data controller.

Funtastic Club is registered with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by us, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. Funtastic club has overall responsibility for ensuring that all our staff complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
The DPO is the first point of contact for individuals whose data the Club processes, and for the ICO.
Our DPO is Régine Natchoo, our club proprietor.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing Funtastic Club of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal date secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way
2. Collected only for valid purpose that we have clearly explained
3. Relevant to the purposes we have told you about and limited to those purposes
4. Accurate and kept up-to-date
5. Kept only as long as necessary for the purposes we have told you about
6. Kept securely

This policy sets out how Funtastic Club aims to comply with these principles.

7. Collecting personal data

We will only process personal data where we have one of the 6 lawful bases to do so under data protection laws:

- The data needs to be processed so that Funtastic Club can fulfil a **contract** with the individual.
- The individual (or their parent/guardian) has freely given clear **consent.**

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first collect it, we will inform the individuals concerned before doing so, and seek consent where necessary.

When the staff no longer need the personal data they hold, they must ensure it is deleted. This will be done in accordance with the appropriate retention timelines.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where it is legally required, or necessary (and it complies with data protection law) we may share information about care recipients (child) with our regulator Ofsted to meet our legal obligation such as safeguarding. We may share with third parties for employment requirements.

We may also share with government bodies where we are required to do so, including for:

- DBS clearance
- Assessment or collection of tax owed to HMRC

We may share personal data with local authorities regarding attendance of the care recipient (child) at the club.

9. Access requests and other Rights of individuals

9.1 Requesting access

The individuals have a right to make a 'subject access request' to gain access to their personal information that Funtastic Club holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purpose of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for

Such request will have to be submitted in writing, either by letter or by email to Funtastic Club. The request should include:

- Name of the individual
- Address
- Contact number and email address
- Details of the information requested

Note that personal data about a child belongs to that child, and not the child's parents or guardian. For a parent or guardian to make an access request with respect to their child, the child must either be unable to understand their rights and the implications of an access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of an access request. Therefore, most access requests from parents or guardian of children attending the club may be granted without the express expression of the child.

9.2 Responding to an access request

We will respond to requests without delay and within 1 month of receipt of the request.
We will provide this free of charge.
We may ask the individual to provide a form of identification.

We will not disclose the information if it:

- Might cause serious harm to the physical or mental health of the child or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.

- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

9.4 Other data protection rights of the individual

In addition to the right to make a subject request and to receive information when we are collecting their data about how we use and process it (section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, delete or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in structured, commonly used format (in certain circumstances).

Individuals should submit any request to the club proprietor responsible. If staff receive such request, they must forward it to the club proprietor.

10. Photographs

As part of our activities, we may take photographs of individuals.

We will obtain written consent from parents/guardians for photographs to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph will be used to both the parent/guardian and child.

Uses may include:

Within the club on display board
Online on our website
Within our Funtastic leaflet

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph and not distribute it further.

When using photographs in this way, we will not accompany them with any other personal information about the child so that they cannot be identified.

11. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against any accidental or unlawful loss, destruction or damage.

In particular:

- Paper based records and portable laptops and hard drives that contain personal data will be locked away when not in use.
- Passwords are used to access laptops and work phones. Staff is reminded to change the password at regular intervals.
- Where we need to share personal data with a third party, we will make sure this information is stored securely and adequately protected.

12. Retention and disposal of records

Personal data will not be held for longer than necessary.

- Child, parents and emergency contact details will be kept for 2 years after the child's last attendance.
- Accident forms will be kept for 21 years and 3 months
- Staff records will be kept for 7 years
- Staff finance records will be kept for 3 years
- All other business records will be kept as per the GDPR guidelines

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely.

13.Personal data breach

We will take all necessary steps to ensure that no personal data breach occur.

In the unlikely event of a suspected data breach, we will follow the procedure described below.

When appropriate, we will report the data breach to the ICO within 72 hours.

Procedure:

Upon finding or causing a breach, or potential breach, the staff member will contact immediately the Data Protection Officer, our club proprietor.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will assess if any personal data has been lost, destroyed, corrupted or disclosed, or if someone accesses the data or passes it on without proper authorisation.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be done on a case by case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g emotional distress) through loss of control over their data, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality or any other significant economic or social disadvantage to the individual concerned.

If it is likely that there is a risk to people's rights and freedoms, the DPO must notify the ICO.

Where the ICO must be notified, the DPO will do this via the 'report a breach pages' on the ICO website within 72 hours.

As required, the DPO will provide the following:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours and explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the information as soon as available.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO must inform those concerned directly in writing and without undue delay. The notification will include:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The DPO will also notify any third parties who can help reduce the loss to individuals such as the police, insurers, professional bodies, or bank or credit card companies.

The DPO will document the facts relating to the breach, its effects and the remedial action taken.

Records of all breaches will be stored safely on our computer system.

Minimising the impact of data breach:

We will endeavour to take the following actions to minimise the risk of a potential data breach:

- All laptops are password protected and are locked away when not in use.
- All paperwork containing personal data is locked away in cupboards
- Shredding of personal data will take place when information no longer needed
- Website: Whilst our website is hosted by a third party, we have a SSL certificate guaranteeing that all data sent via our website is encrypted. We have also full control over all the information that is published. Therefore, if there was a case where certain data was published inappropriately, it could be taken down immediately.

14.Training

All staff will be provided with data protection training as part of their induction process. Ongoing training will take place to accommodate any changes in legislation.

15. Review of the Policy

This policy will be reviewed on a yearly basis by the DPO.

16.Links with other policies

This data protection policy is linked with our confidentiality policy.