The JR Sports Group

Data Protection Policy

Signed: James Richardson

The JR Sports Group Director

26/06/2023

Revision History

Revision	Nature of Changes	Made by	Date	Signed Off
1	Original Release	JR	26/06/23	James Richardson
2	Process Updates	LO	15/11/23	James Richardson

INTRODUCTION

The JR Sports Group may have to collect and use information about people with whom we work and provide services for. 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. This Data Protection Policy outlines the principles and guidelines followed by The JR Sports Group, a children's sports coaching company, to ensure the protection of personal data collected, processed, and stored. We are committed to safeguarding the privacy of individuals, especially children, and complying with applicable data protection laws and regulations. This policy serves as a foundation for our data protection practices and applies to all employees, contractors, and third parties working on behalf of The JR Sports Group. The JR Sports Group will comply with all applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA), and any other relevant local, state, or national laws pertaining to data protection and privacy.

SCOPE

This policy applies to all personal data processed by The JR Sports Group, including but not limited to data collected from children, parents, guardians, and employees. It covers both electronic and physical data and encompasses all systems, processes, and procedures employed by The JR Sports Group for collecting, storing, using, disclosing, and disposing of personal data.

DEFINITIONS

“Personal data” is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

An individual about whom such information is stored is known as the **“Data Subject”**. It includes but is not limited to employees.

“Data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A **"data controller"** determines the purposes and means of processing personal data. In other words, the data controller decides the how and why of a data processing operation.

"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

DATA PROTECTION 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. The lead person responsible for data protection is the Director and **Data Protection Officer James Richardson - 07878988550 or james@jrsportsgroup.com.** The DPO and the Operations Manager Lucy Osborn are responsible for reviewing and auditing our data protection systems.

COLLECTION AND USE OF PERSONAL DATA

Consent and Privacy Notices

a) Consent will be obtained from parents, guardians, or legal representatives before collecting personal data of children.

b) Clear and concise privacy notices will be provided, explaining the purpose, legal basis, and retention period for collecting and using personal data.

c) Privacy notices will be readily accessible and written in clear language suitable for the understanding of parents or guardians.

Minimisation of Data

a) Only necessary personal data will be collected, limited to what is required for the provision of coaching services and fulfilling legal obligations.

b) Data collected will be relevant, accurate, and up to date.

c) Excessive data will not be requested or stored.

Purpose Limitation

a) Personal data will only be used for the specified purposes for which it was collected unless consent is obtained for alternative uses.

b) Personal data will not be used for any purpose incompatible with the original collection without obtaining appropriate consent or complying with legal requirements.

Safeguards

a) Appropriate technical and organisational measures will be implemented to protect personal data against unauthorised access, loss, disclosure, alteration, or destruction.

b) Physical, technical, and administrative controls will be employed to ensure data security.

c) Access to personal data will be restricted to authorised personnel on a need-to-know basis.

DATA BREACHES

This breach procedure sets out the course of action to be followed by all staff at The JR Sports Group if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Breach Categories:

Data protection breaches may arise from various sources, encompassing scenarios such as the loss or theft of staff equipment storing data, inappropriate access controls, equipment failure, inadequate data destruction procedures, human error, cyber-attacks, and hacking.

Managing a Data Breach:

Upon the identification or notification of a personal data breach, specific steps must be taken:

1. The individual discovering or receiving a report of a breach must promptly inform the Data Protection Officer (DPO), even if the incident occurs outside regular working hours. Completion of a reporting form is imperative.

2. The DPO needs to swiftly determine if the breach is ongoing and take immediate measures to minimise its impact, which could involve actions like system shutdowns.

3. It is the responsibility of the DPO to initiate appropriate actions and conduct a thorough investigation.

4. The DPO must consider whether involving law enforcement, particularly the police, is necessary, especially if illegal activity is suspected or known. Legal support from the company should be sought in such cases.

5. Rapid steps should be taken by the DPO to recover losses and mitigate damage, including attempts to recover lost equipment, communication with affected parties, and the use of backups to restore data.

Investigation:

Following the identification of a breach, the subsequent stage typically involves a comprehensive investigation by the DPO. This investigation should delve into various aspects, including:

- The type and sensitivity of the compromised data.

- The adequacy of existing protections, such as encryption.

- The specific events surrounding the data breach and its potential for illegal or inappropriate use.

- The number and types of individuals affected, considering categories like children, staff members, and suppliers.

- Wider consequences resulting from the breach.

Notification:

Notification processes are crucial and necessitate careful consideration. Key points include:

- Determining who should be notified, following an initial investigation.

- In significant breaches, notifying the Information Commissioner's Office (ICO) within 72 hours is mandatory.

- Providing clear and specific advice to individuals on actions they can take to protect themselves and the company's efforts to assist them.

- Offering individuals the opportunity to file a formal complaint, adhering to the company's Complaints Procedure.

Review and Evaluation:

Once the immediate aftermath of a breach subsides, the DPO should conduct a comprehensive review. This involves assessing the root causes of the breach, evaluating the effectiveness of the response, and, if necessary, formulating an action

plan to address systemic or ongoing problems. Collaboration with human resources or internal audit may be necessary for disciplinary investigations. Additionally, periodic reviews of the breach procedure may be required in response to a breach, legislative changes, new case law, or updated guidance.

Implementation:

Critical to breach prevention is ensuring that all staff are well-informed about the company's Data Protection policy and the associated breach procedure. This education should be integrated into induction, supervision, and ongoing training. Staff with queries or uncertainties about the company's Data Protection policy should actively engage with the DPO for clarification and guidance.

DATA RETENTION/STORAGE PERIOD

Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected, including any legal, accounting, or reporting requirements. Data will be securely disposed of once the retention period expires.

Employee Data:

Personal data of employees will be securely destroyed upon their departure from The JR Sports Group.

Children/Parents Data:

1. Active Participants:

Data of children and their parents actively enrolled in our programs will be retained on our booking system for the duration of their participation.

2. Inactive Participants:

For children and parents who are no longer attending our programs, their data will be retained for a period of one year after their last engagement. This allows for potential re-enrollment in annual camps or other activities.

3. Data Removal Requests:

Individuals have the right to request the removal of their data at any time. Upon receiving such a request, the relevant data will be promptly deleted from our systems.

DATA SUBJECT RIGHTS/DISCLOSURE PROCESS

Data Subject Rights

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the company handles their personal data are set out below:

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the company's processing activities;

(c) Request access to their personal data that we hold

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for

which it was collected or processed or to rectify inaccurate data or to complete incomplete

data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the DPO to verify the identity of the individual making the request.

Subject Access Requests

According to Data Protection Law, individuals have a fundamental entitlement to ascertain whether a company possesses or processes their personal data, to obtain access to such data, and to receive additional details. This entitlement is commonly referred to as the right of access or the right to submit a data subject access request (SAR).

The company is obligated to provide the data subject with the following information:

(a) Confirmation of the processing of their data;

(b) Access to their personal data;

(c) An explanation of the data being processed;

(d) The purpose for processing the information;

(e) The recipients or categories of recipients to whom the information may be disclosed;

(f) Information about the sources from which the company obtained the data;

(g) Regarding any personal data processed to assess matters concerning the data subject, forming the sole basis for a decision significantly impacting them, an explanation of the logic behind the Data Controller's decision-making. This may

encompass, but is not limited to, factors such as work performance, creditworthiness, reliability, and conduct;

(h) Additional supplementary information.

How to Recognise a Subject Access Request

A data subject access request is a formal inquiry initiated by an individual or an authorised representative (e.g., solicitor or parent on behalf of a child), seeking confirmation on whether the company processes personal data related to the individual. If confirmed, the request aims to obtain access to the personal data and supplementary information. A valid request can be submitted in writing (letter, email, WhatsApp) or verbally (e.g., during a telephone conversation) and may reference the UK GDPR, 'data protection,' or 'personal data,' though such mention is not mandatory. It's important to note that, generally, a data subject is entitled to access only their own personal data, not information about other individuals.

How to Make a Data Subject Access Request

Although it is not obligatory, we recommend individuals interested in making a request to submit it in writing, specifying the exact personal data they seek. This approach helps the company promptly identify your intention to initiate a data subject access request and the specifics of your inquiry. In cases where the request lacks clarity or is vague, we may need to seek clarification on the request's scope, potentially causing a delay in commencing the processing period for the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the DPO.

Acknowledging the Request

When receiving a SAR the company shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request. In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);

- further clarification about the requested information;

- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information;

- consent (if requesting third party data).

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before addressing a SAR, the company will reasonably verify the requester's identity, typically straightforward for current employees. The company may request additional information to confirm the requestor's identity and may accept documentation like a passport, driving licence, utility bill, birth/marriage certificate, credit card, or mortgage statement if doubts arise. If a large data volume is requested, the company may seek additional details to clarify the request, but the purpose behind the request will not be questioned. The company promptly informs the requester if more information is required, and the response period starts upon receipt of the additional information.

Requests Made by Third Parties or on Behalf of Children

The third party requesting personal data on behalf of an individual must demonstrate their entitlement to act on the individual's behalf. This can be through a written authorization or a general power of attorney. Proof of identity may be required in certain situations. If there is any doubt or concern about providing the data to the third party, the company should furnish the information directly to the data subject. The data subject can then decide whether to share the information with the third party.

When requests are made on behalf of children, it's crucial to recognize that even if a child doesn't fully grasp subject access rights, the right belongs to the child, not the parent or guardian. Before responding to a request regarding a child, the company should assess the child's maturity to understand their rights. If confident, the company should usually respond directly to the child or seek their consent before releasing information.

For a child aged 12 or older, the company presumes they have the capacity to exercise their right of access. If the child is deemed capable and there is no reason to believe otherwise, the company requires the child's written authorization before responding to the requester or providing personal data directly. The company may also refuse to provide information to parents if it could harm the child.

Time Period for Responding to a SAR

The company must respond to a SAR within one calendar month, starting from the day of request receipt or the day additional identification, information, or required fees are received. If there's reasonable doubt about the requestor's identity, the response period begins only when sufficient identification details are provided, and for third-party requests, written authorisation from the data subject is received.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right: to request that the Company rectifies, erases or restricts the processing of his personal data, to object to its processing; to lodge a complaint with the ICO;
- where the personal data has not been collected from the individual, any information available regarding the source of the data;
- any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

Record Keeping

A record of all subject access requests shall be kept by the DPO. The record shall include the date the SAR was received, the name of the requester, what data the company sent to the requester and the date of the response.

THIRD PARTY DISCLOSURES

a. Personal data will not be disclosed or shared with third parties without the explicit consent of parents, guardians, or legal representatives, except where required by law or to fulfil contractual obligations.

b. Contracts and agreements will be established with third-party service providers to ensure their compliance with data protection laws and regulations.

EMPLOYEE TRAINING AND RESPONSIBILITY

a. Employees and contractors will be trained on data protection policies, procedures, and best practices.

b. Regular training programs will be conducted to keep staff updated on relevant data protection laws and regulations.

c. Employees and contractors will be responsible for adhering to this Data Protection Policy and maintaining the confidentiality and security of personal data.

DATA AUDITING AND MONITORING PROCESS

Overview

The JR Sports Group is committed to safeguarding the personal information of children, parents, staff, and service providers entrusted to us. To maintain the highest standards of data protection, we implement a robust auditing and monitoring process. This process ensures the secure handling, storage, and processing of personal data in accordance with relevant data protection laws.

Data Audit Schedule

Regular audits will be conducted to review and assess the handling of personal data within our organisation. These audits will be scheduled annually and will cover all aspects of data processing activities.

Data Protection Officer (DPO) Responsibilities

Our designated Data Protection Officer (DPO) will oversee the data auditing and monitoring process. The DPO is responsible for coordinating and conducting audits, ensuring compliance with data protection policies, and addressing any identified issues promptly.

Audit Criteria

The audits will focus on, but not be limited to, the following criteria:

a. Data Collection: Verify that only necessary and relevant data is collected for specified purposes.

b. Consent Management: Confirm that valid consent is obtained for the processing of personal data, especially in the case of children.

c. Data Security: Assess the effectiveness of security measures in place to protect personal data from unauthorised access, disclosure, alteration, or destruction.

d. Data Accuracy: Ensure that personal data is accurate, up-to-date, and corrected promptly in the event of inaccuracies.

e. Data Retention: Confirm that data is retained only for the necessary duration and is securely disposed of when no longer required.

Audit Reporting

Following each audit, a detailed report will be compiled, outlining findings, recommendations, and actions taken or planned to address any identified issues.

Continuous Monitoring

In addition to scheduled audits, continuous monitoring mechanisms will be implemented to identify and address any potential data protection risks in real-time.

Policy Review and Updates

This Data Protection Policy will be reviewed periodically to ensure its continued relevance and compliance with evolving legal and regulatory requirements. Updates may be made as necessary, and employees will be notified of any changes.

By implementing and adhering to this Data Protection Policy, The JR Sports Group demonstrates its commitment to protecting the personal data of children and their families while providing quality sports coaching services.