



Creative Sports Coaching CIC

Data Protection Policy and Privacy Notices

1. Aims

Our company aims to ensure that all personal data collected about staff, participants, parents, stakeholders, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the [Data Protection Act 2018 \(DPA 2018\)](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to the use of biometric data.

3. Definitions

3.1 Personal data

Any information relating to an identified, or identifiable, living individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

3.2 Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns) where used for identification purposes
- Health - physical or mental
- Sex life or sexual orientation

3.3 Processing

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

3.4 Data subject

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

3.5 Data controller

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

3.6 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.

3.7 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

Our company processes personal data relating to parents, participants, staff, stakeholders, visitors and others, and therefore is a data controller.

5. Roles and responsibilities

This policy applies to all staff employed by our company, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing body

The company Directors have overall responsibility for ensuring that our company complies with all relevant data protection obligations.

5.2 Data protection officer

The company Directors (DPO) are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities, where relevant and is also the first point of contact for individuals whose data the company processes.

Our DPO is James Hatch and is contactable via email James@creativesportscoaching.co.uk

5.3 Company Directors

The company Directors acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for collecting, storing and processing any personal data in accordance with this policy and informing the company of any changes to their personal data, such as a change of address. They are also responsible for 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 data 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, or transfer personal data outside the European Economic Area.

- 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

The GDPR is based on data protection principles that our company must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the company aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the company can **fulfil a contract** with the individual, or the individual has asked the company to take specific steps before entering into a contract.
- The data needs to be processed so that the company can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
- The data needs to be processed so that the company, as a public authority, can **perform a task in the public interest or exercise its official authority**.
- The data needs to be processed for the **legitimate interests** of the company (where the processing is not for any tasks the company performs as a sole trader) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when in the case of a participant) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer in the case of a participant) has given **explicit consent**.
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer in the case of a participant) has given **consent**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.

- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

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 obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the company's knowing.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a participant or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies (we will seek consent as necessary before doing this)
- Our suppliers or contractors need data to enable us to provide services to our staff and participants, for example IT companies.*

* When doing this, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law.
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes 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, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject 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 a subject access request. Therefore, most subject access requests from parents or carers of participants at our sessions may be granted without the express permission of the participant. This is not a rule and a participant's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the participant or another.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see records of their child

Parents, or those with parental responsibility, have a legal right to free access to their child's records (which includes most information about a participant) within 15 working days of receipt of a written request. If the request is for a copy of the records, the company may charge a fee to cover the cost of supplying it.

This right applies as long as the participant concerned is aged under 18. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the participant or another individual.

11. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our sessions. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent /carer and participant.

Any photographs and videos taken by parents/carers at our events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other participants are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the company takes photographs and videos, uses may include:

11.1 Within the company on boards and in promotional brochures, newsletters, etc.

11.2 Outside of our activities by external agencies such as the photographers, newspapers and any campaigns

11.3 Online on our company website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- 12.1** Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their knowledge.
- 12.2** Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- 12.3** Completing data protection impact assessments where the company's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- 12.4** Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- 12.5** Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters. We will also keep a record of attendance.
- 12.6** Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- 12.7** Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply.
- 12.8** Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our company and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

13. 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 accidental or unlawful loss, destruction or damage. In particular:

- 13.1** Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- 13.2** Papers containing confidential personal data must not be left on office and working desks, on tables, or left anywhere else where there is general access.
- 13.3** Where personal information needs to be taken off site, staff must sign it in and out after speaking with the company Director.
- 13.4** Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and participants are reminded that they should not reuse passwords from other sites.
- 13.5** Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- 13.6** Staff or participants who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment
- 13.7** Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

14. Disposal of records

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, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the company's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The company will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours of becoming aware of it. A non-anonymised dataset being published on the company's website

15.1 Safeguarding information being made available to an unauthorised person

15.2 The theft of a company laptop containing non-encrypted personal data about participants

16. Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the company's processes make it necessary.

17. Monitoring arrangements

This policy was approved by the company Director in September 2024. It will be reviewed every two years or earlier if changes need to be made.

Appendix 1

Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

3. Staff will co-operate with the investigation, including allowing access to information and responding to questions. The investigation will not be treated as a disciplinary investigation.

4. If a breach has occurred or it is considered to be likely that is the case, the DPO will notify the company Directors

5. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary.

6. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

7. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#).

8. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

9. Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through their breach report line (0303 123 1113), within 72 hours of the company's awareness of the breach. As required, the DPO will set out:

- 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 DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

10. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the company's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

11. Where the company is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

12. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

13. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts relating to the breach
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored by the company..

14. The DPO and company Director will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible.

15. The DPO and company Director will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the company to reduce risks of future breaches.

Appendix 2

Privacy Notice for Parents

Introduction

Under data protection law, individuals have a right to be informed about how the company uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about pupils. We, Creative Sports Coaching CIC, are the 'data controller' for the purposes of data protection law. Our data protection officer is James Hatch (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Participant records
- Characteristics, such as ethnic background, eligibility for projects, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

We may also hold data about participants that we have received from other organisations, including other companies, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support participant learning
- Monitor and report on participant progress
- Provide appropriate care
- Protect participant welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use participants' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process participant's ' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use participant's personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using participants' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about participants is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about participants while they are attending our activities. We may also keep it beyond their attendance at our activities if this is necessary in order to comply with our legal obligations.

Data sharing

We do not share information about participants with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about participants with:

- Our local authority
- The Department for Education
- The pupil's family or representatives
- Our official regulator
- Suppliers and service providers
- Health authorities
- Health and social welfare organisations

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them. Parents can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the company holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request please contact our data protection officer

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer, James Hatch, on 07711270986.

Appendix 3

Privacy Notice for Pupils

Introduction

You have a legal right to be informed about how our company uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you. We, Creative Sports Coaching CIC, are the 'data controller' for the purposes of data protection law. Our data protection officer is James Hatch (see 'Contact us' below).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at our sessions. This information includes:

- Your contact details
- Your reports
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Photographs

Why we use this data

We use this data to help run the company effectively, including to:

- Get in touch with you and your parents when we need to
- Check if there is any need of any extra help
- Track how well you are performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest

Sometimes, we may also use your personal information where:

- You, or your parents have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent. Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data. We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a participant at our activities. We may also keep it after you have left our activities, where we are required to by law.

Data sharing

We do not share personal information about you with anyone outside the company without permission from you or your parents, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may also share personal information about you with:

- Our local authority
- Your family or representatives
- Our official regulator
- Suppliers and service providers
- Health authorities
- Health and social welfare organisations

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a 'subject access request', as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances. If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer, James Hatch, on 07711270986.

Appendix 4

Privacy Notice for Staff

Introduction

Under data protection law, individuals have a right to be informed about how the company uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our company. We, Creative Sports Coaching CIC, are the 'data controller' for the purposes of data protection law. Our data protection officer is James Hatch (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our company.

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a covering letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and /or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- Data about your use of the company's information and communications system

We may also collect, store and use information about you that falls into 'special categories' of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the company, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards participants
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so. Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the company's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying) or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended, we will delete this file.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority
- The Department for Education
- Your family or representatives
- Our official regulator
- Suppliers and service providers
- Trade unions and associations
- Health authorities
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer, James Hatch, on 07711270986.