Little Gems
Wellbeing Centre

GDPR / Data Protection Policy V2

Introduction

We collect and use certain types of personal information about the following categories of individuals:

- Staff and volunteers that or employed, work or volunteer with us
- Professional advisers and service providers, including providers of book-keeping, banking and management services
- Clients that take part or use the coaching, riding and other service that we provide

We will process this personal information in the following ways:

- Collect the full names, email addresses, workplace addresses and other necessary contact details such as telephone numbers of the categories of individuals listed above. This information shall be held and controlled for the legitimate processing of such data to ensure effective communications in the reasonable pursuance of our business activities
- Undertake other processing when required to comply with statutory and other legal obligation

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (the "GDPR") and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

The GDPR applies to computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable based on specific criteria (so you would be able to use something like the individual's name to find their information) and, if this is the case, it does not matter whether the information is located in a different physical location.

Review Arrangements

The policy will be reviewed every three years, or in the following circumstances:

- Changes in legislation and/or government guidance
- As a result of any other significant change or event
- To reflect best practice

Responsibilities

For the purposes of the Data Protection Act 2018 and the UK GDPR, where we provide goods and services to a resident of the UK, we will appoint:

• A Data Protection Officer who is responsible for oversight of data protection processes

Little Gems Wellbeing Centre Ltd Data protection officer is Hayley James

Personal Data

'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or obtain. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:
• Personal data revealing racial or ethnic origin
• Personal data revealing political opinions
• Personal data revealing religious or philosophical beliefs
• Personal data revealing trade union membership
• Genetic data
• Biometric data (where used for identification purposes)
• Data concerning health
• Data concerning a person's sex life
• Data concerning a person's sexual orientation.

Special category information is given special protection, and additional safeguards apply if this information is to be collected and used. We will only collect or process special category personal data or information where this is needed to ensure our services are delivered with due cognizance of the need to ensure Equality, Diversity and Inclusivity.

The Data Protection Principles

We will follow the six data protection principles as laid down in the GDPR:
• Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met
• Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes
• Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed
• Personal data shall be accurate and, where necessary, kept up to date
• Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes
• Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction, or damage, using appropriate technical or organisational measures

In addition to this, we are committed to always ensuring that anyone dealing with personal data is mindful of the individual's rights under the law (as explained in more detail below). We are committed to always complying with the data protection principles. This means that we will:

- Inform individuals as to the purpose of collecting any information from them, as and when we ask for it
- Be responsible for checking the quality and accuracy of the information
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the records retention policy • Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times
- Share personal information with others only when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access requests
- Report any breaches of the GDPR in accordance with the procedure detailed below

Conditions for Processing in the First Data Protection Principle

We will esnure:

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request
- The processing is necessary for the performance of a legal obligation to which we are subject
- The processing is necessary to protect the vital interests of the individual or another
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us
- The processing is necessary for a legitimate interest of us or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

Disclosure of Personal Data

The following list includes the most usual reasons that we will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former trustee, employee or volunteer
- For the prevention or detection of crime
- For the assessment of any tax or duty
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the us
- For, or in connection with, legal proceedings (including prospective legal proceedings) • For obtaining legal advice
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
- Any investigation by a statutory authority or regulator

We may receive requests from third parties (i.e. those other than the data subject, us, and its professional advisers and service providers) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR, which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or us.

Requests for the disclosure of personal data must be sent to:
Name: Lorraine Webster (Proprietor) who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

Security of Personal Data

We will take reasonable steps to ensure that managers, employees, volunteers and thirdparty advisers and service providers will only have access to personal data where it is necessary for them to carry out their duties. All such persons will be made aware of this Policy and their duties under the GDPR. We will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Subject Access Requests

Anybody who makes a request to see any personal information held about them by us in making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, if they constitute a "filing system" (see above).

All requests should be sent to the person named above, within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

Any individual may appoint another person to request access to their records. In such circumstances then we must have written evidence that the individual has authorised the

person to make the application and then we must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A subject access request must be made in writing. We may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the person named above before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Exemptions to Access by Data Subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

Other Rights of Individuals

We have an obligation to comply with the rights of individuals under the law and we take these rights seriously. The following section sets out how we will comply with the rights to:

- Object to processing
- Rectification
- Erasure
- Data portability

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the person named above within 2 working days of receipt. We will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The person named above will be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay.

Where any request for rectification is received, it should be sent to the person named above within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the complaint's procedure, or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to Erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed
- Where consent is withdrawn and there is no other legal basis for the processing
- Where an objection has been raised under the right to object, and found to be legitimate
- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met)
- Where there is a legal obligation on us to delete

The person named above will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other

controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made. **Right to Restrict Processing**

In the following circumstances, processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested, during the period when we are attempting to verify the accuracy of the data
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim
- Where there has been an objection made, pending the outcome of any decision

Right to Portability

If an individual wants to send their personal data to another organisation they have a right to request that you provide their information in a structured, commonly used, and machine readable format. If a request for this is made, it should be forwarded to the person named above within 2 working days of receipt. They will review and revert as necessary.

Breach of any Requirement of the GDPR

Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the person named above.

Once notified, they will assess:

- The extent of the breach
- The risks to the data subjects because of the breach
- Any security measures in place that will protect the information
- Any measures that can be taken immediately to mitigate the risk to the individuals

Unless the person named above concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to our attention, unless a delay can be justified.

The Information Commissioner shall be told:

- Details of the breach, including the volume of data at risk, and the number and categories of data subjects • The contact point for any enquiries
- The likely consequences of the breach
- Measures proposed or already taken to address the breach

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the person named above shall notify data subjects of the breach without

undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- The nature of the breach
- Who to contact with any questions
- Measures taken to mitigate any risks.

The person named above shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented, including the implementation of additional training.

Destruction of data

Excluding accident forms which will be kept indefinitely, all other paper student data will be destroyed 4 months after the end of contract, unless any information is highlighted as needing to be kept for any ongoing scenario. All information on the "academy" student manager app will be stored/destroyed via their GDPR/data protection policy.

Contact

If anyone has any concerns or questions in relation to this policy they should contact us using the contact information on our website.

Signed:

Name: Hayley James (Manager)

Date: 10 / 02 / 2025