Changing Chances Ltd

Data protection (GDPR) policy.

The purpose and scope of this policy

Changing Chances Ltd delivers services including training and coaching for children and young people and for their parents, carers, teachers and other professionals working with children. Across the scope of its work, Changing Chances Ltd ("the Company") is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our directors, staff, associates, clients, suppliers and other individuals in order to operate and perform legitimate business.

This policy sets out how we seek to protect personal data and ensure that staff and associates understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff and associates to ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity begins to ensure that relevant compliance steps are followed.

Scope

This policy applies to all directors, staff and associates of the Company. You must be familiar with this policy and comply with its terms. This policy supplements our privacy policy. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to all directors, staff and associates before being adopted.

Who is Responsible for this policy?

Alison Rendle (Director) acts as Data Protection Officer (DPO) for Changing Chances Ltd and as such has overall responsibility for the day-to-day implementation of this policy.

The Principles

The Company shall comply with the principles of data protection enumerated in the current General Data Protection Regulation (2018). We will make every effort possible in everything we do to comply with these principles:

- **Lawful, Fair and Transparent:** data collection must be fair, for a legal purpose and we must be open and transparent about how the data will be used
- **Limited for its Purpose:** data can only be collected for a specific purpose
- **Data Minimisation:** any data collected must be necessary and not excessive for its

purpose

- **Accurate:** the data we hold must be accurate and kept up to date
- **Retention:** we cannot store data longer than is necessary and in line with our prime's contractual specifications
- **Integrity and Confidentiality:** the data we hold must be kept safe and secure and in line with our prime's contractual specifications

Our Procedures

Fair and Lawful Processing:

The Company will process personal data fairly and lawfully in accordance with individuals' rights. This means that we should not process personal data unless the individual whose details we are processing has actively consented to this happening.

Lawful Basis for Processing Data:

At least one of the following conditions must apply whenever we process personal data:

- **Consent:** we must hold recent, clear, explicit and defined consent for the individual's data to be processed for a specific purpose.
- **Contract:** the processing is necessary to fulfil or prepare a contract for the individual.
- **Legal Obligation / Public Function:** we have a legal obligation to process the data (excluding a contract) or it is necessary for a public interest that is clearly based in law.
- **Vital Interests:** processing the data is necessary to protect a person's life in a medical situation.
- **Legitimate Interests:** for delivery of services but will not prejudice the individual's privacy.

At Changing Chances, we will ensure that the processing of any data will be of lawful basis and necessary to deliver our services as well as in our legitimate interest. In most cases, these provisions will apply to routine business data processing activities.

Special Categories of Personal Data

In most cases where we process special categories of personal data (previously known as sensitive personal data), we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Responsibilities of the Data Protection Officer

- Maintaining the appropriate registration with the Information Commissioner's Office
- Keeping the Directors updated about data protection responsibilities, risks and issues

- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all directors, staff, associates and those included in this policy
- Answering questions on data protection from directors, staff, associates and other stakeholders
- Responding to individuals such as clients and associates who wish to know what data is being held on them by Changing Chances Ltd
- Checking and approving with third parties that handle the Company's data any contracts or agreement regarding data processing
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Ensuring all marketing initiatives adhere to data protection laws and the Company's GDPR Policy
- Ensuring all systems, services, software and equipment meet acceptable security standards

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this, or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate, you should record the fact that the accuracy of the information is disputed and inform the DPO immediately. The DPO will investigate your concerns and respond in writing to you without unnecessary delay.

Data Security

All directors, staff and associates must keep personal data secure against loss or misuse at all times. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot gain access
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks must be locked away securely when they are not being used

- Data should be regularly backed-up
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall
- All possible technical measures must be put in place to keep data safe

Data Retention

The Company will normally retain personal data for cognitive assessments, coaching, training, finance, client data and HR.

What it is necessary to retain will depend on the circumstances of each case, the reasons that the personal data was obtained should be taken into account, but decisions must always be determined in a manner consistent with our data retention guidelines. No data will be retained if it is subject to a 'Right to Erasure' request, unless it would be unlawful for us to delete such data.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO. To the best of our knowledge, there is currently no requirement for the Company or its representatives to transfer data outside the UK.

Rights of Individuals

Individuals have rights to their data which the Company must respect and comply with to the best of our abilities. The Company must ensure individuals can exercise their rights in the following ways:

- **Right to be Informed:** providing privacy notices that are transparent, intelligible, accessible and free of charge and are written in clean language detailing how and why we will be using their personal data
- **Right of Access:** enabling individuals to access their personal data and any supplementary information. Allowing individuals to be aware of and verify the lawfulness of the processing activities
- **Right to Rectification:** we must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This must be done without delay and no later than within one month of the request. This can be extended to two months with permission from the DPO
- **Right to Erasure:** we must delete an individual's data if requested and there is no compelling reason for its continued processing. The Company reserves the right to deny a request to erasure if there is a lawful reason that the data should be kept
- **Right to Restrict Processing:** we must comply with any request to restrict, block or

otherwise suppress the processing of personal data. We can store restricted personal data but must not process it further. We must retain enough data to ensure that the right to restriction is respected in the future

- **Right to Data Portability:** if requested by the individual, we must provide individuals with their data so that they can re-use it for their own purposes or across different services.
- **Right to Object:** we must respect the rights of an individual to object to data processing based on legitimate interest to the performance of a public interest task: to direct marketing including profiling; to processing their data for scientific or historical research and statistics
- **Rights in Relation to Automated Decision Making and Profiling:** we must respect the rights of individuals in automated decision making and profiling. Individuals retain the right to object and to request human intervention

Subject Access Requests

We must provide an individual with a copy of the information we hold about them free of charge. This must occur without delay and within one month of receipt of verification of their identity. If it is complex, this can be extended to two months with the DPO's approval.

Once a data access request has been made, the Company will not change or amend any data that has been requested. Doing so is a Criminal Offence.

Data must be provided in a commonly used electronic format.

The Company can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can ask the individual to specify the information that they are requesting. This can ONLY be done with the express permission of the DPO.

Data Portability Requests

The Company must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file. We must provide this information to the individual or to the Data Controller that they have requested it be sent to. This must be done free of charge and without delay, taking no longer than one month. This can be extended to two months if the data is complex, the individual informed and approval granted by the DPO.

Right to Erasure

Individuals have a right to have their data erased and for process to cease in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected and /or processed
- where consent is withdrawn
- where the individual objects to processing and there is no over-riding legitimate interest for continuing the processing

- where the personal data was unlawfully processed or otherwise breached data protection laws
- to comply with a legal obligation
- when the processing relates to a child
- if personal data that needs to be erased has been passed to third parties, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The Company can only **refuse** to comply with a right to erasure in the following circumstances:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- the exercise or defence of legal claims

Right to Object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless we have legitimate grounds which override the interests, rights and freedoms of the individual, or the processing relates to the establishment, exercise or defence of legal claims.

Right to Restrict Processing

Individuals have the right to request that their data be, restricted, blocked or otherwise suppressed for the processing of personal data. Data will be extracted from the database and held in a secure format until such time as the dispute is resolved. The Company must retain enough data to ensure that the right to restriction is respected in the future.

Right to Restrict Automated Profiling or Decision Making

The Company does not carry out automated profiling or decision making.

Our Terms of Business contains a Privacy Notice to clients on data protection. This notice:

- sets out the purposes and lawful basis for which we hold personal data on customers, employees and associates
- high-lights that our work may require us to give information to third parties such as other professional advisers
- explains that customers have a right of access to the personal data that we hold about them and the right to withdraw or object at any time
- provides details of how to contact our DPO and how to make a complaint

Third Parties

The Company has written contracts in place with all of our third parties that contain a clause setting out their liabilities, obligations and responsibilities. We will only appoint processors who can provide sufficient guarantees under GDPR that the right of the data subjects will be respected and protected. When processing data subjects, we will only act on the documentation of the Controller and acknowledge our responsibilities under GDPR. We will protect and respect the rights of data subjects.

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. The Company will not keep a record of data relating to criminal offences. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. Approval to carry out a criminal records check is granted by the DPO, in accordance with the Rehabilitation of Offenders Act 1974.

Audits, Monitoring and Training

Data Audits

Regular data audits will be carried out to manage and mitigate risks and inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and retention timescales.

Monitoring

All employees and associate of the Company must observe and comply with this policy at all times. The DPO has overall responsibility for this policy and the Company will keep this policy under review and amend as and when it is required. The DPO must be notified of any breaches of this policy without delay.

Training

All directors, staff and associates will receive training on this policy. New joiners will receive training as part of the induction process. Training will cover:

- the law relating to data protection
- our data protection and related policies and procedures

Reporting Breaches

Any breach of this policy or of the Data Protection Laws must be reported to the DPO as soon as practically possible, this means as soon as you have become aware of a breach. The Company has a legal obligation to report any data breaches to the relevant prime / authority within 72 hours.

All directors, staff and associates have an obligation to report actual or potential data protestation compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Policy updated: 4th June 2021