MAHDLO

An OnSide Youth Zone

DATA PROTECTION & RETENTION POLICY

Document Control

Document Developed by:	HR
Date:	June 2022
Version number:	4
For further information:	Chief Executive Officer
Review date:	June 2023

1.0 Policy Statement

Mahdlo (Oldham Youth Zone) is committed to protecting personal data and respecting the rights of the people whose personal data we collect and use (data subjects). This policy explains our responsibilities and how we will comply with the General Data Protection Regulation (GDPR).

Personal data is defined as that which relates to an identifiable living individual and includes any expression of opinion about that individual. Within Mahdlo, personal data includes information about job applicants, employees, volunteers, beneficiaries, donors, trustees, such as name and address.

We process personal data to:

1. maintain our contacts held on Salesforce (Mahdlo's CRM database)
2. recruit, support and manage staff and volunteers
3. safeguard children and young people at risk
4. maintain our HR and financial records held on hard files and electronic databases KRONOS and ADP iHCM (Mahdlo's Time and Attendance Management system and Payroll system respectively)
5. recruit and support trustees
6. provide services to our Youth Zones
7. undertake research
8. respond effectively to enquiries and any complaints
9. communicating with our supporters

2.0 The Principles

2.1 We are committed to protecting personal data from being misused, shared inappropriately or being inaccurate.

We will ensure all personal data is:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date, where necessary;
5. kept for no longer than is necessary where data subjects are identifiable;
6. processed securely and protected against accidental loss, destruction or damage;
7. processed in keeping with the rights of data subjects regarding their personal data.

2.2 Data subjects, including employees, have the:

1. right to be informed about the processing of their personal data;
2. right to rectification if their personal data is inaccurate or incomplete;
3. right of access to their personal data and supplementary information, and the right to confirmation that their personal data is being processed;
4. right to be forgotten by having their personal data deleted or removed on request where there is no compelling for an organisation to continue to process it;
5. right to restrict processing of their personal data, for example, if they consider that processing is unlawful or the data is inaccurate;
6. right to data portability of their personal data for their own purposes (they will be allowed to obtain and reuse their data);

7. right to object to the processing of their personal data for direct marketing, scientific or historical research, or statistical purposes.

3.0 Application of the Policy

3.1 The Data Protection Policy applies to:

- successful and unsuccessful applicants, and former applicants (see appendix 2 for the Applicant Privacy Notice)
- current and former employees which includes full time, part-time, sessional, casual employees and contract workers, as well as volunteers
- young people – current and former members as well as visitors
- both manual and electronic records

3.2 Mahdlo's employees, trustees and volunteers who process personal information are required to read, understand and comply with this policy. Any individual who breaches the policy may be subject to disciplinary action. If you are unsure about whether anything you plan to do, or are currently doing, may breach this policy you must first speak to HR.

3.3 Data subjects of Mahdlo will have their personal data processed in line with this policy.

3.4 Organisations, consultants and other third parties appointed to undertake services for Mahdlo are required to comply with this policy as a condition of their contract. Any breach of the policy will be taken seriously and could result in Mahdlo terminating the contract.

3.5 Training will be provided by Mahdlo, as and when appropriate, for employees, trustees and volunteers to ensure an understanding of the policy and its application to our work.

4.0 Personal Data

4.1 Mahdlo will collect and process personal data about a wide range of data subjects. This includes data received directly from individuals and from other sources. The personal data processed will be in both electronic and paper form and will include the following:

1. CVs, application forms, shortlisting and interview notes, references, etc. obtained during selection processes
2. terms of employment
3. payroll information including tax, national insurance details and dates of birth
4. emergency contacts
5. health and sickness absence records
6. information about performance, behaviours and achievements
7. details of any disciplinary investigations and proceedings
8. training and development records
9. contact names, addresses, telephone numbers and email addresses
10. visual images
11. personal and demographic information (date of birth, age, gender, nationality, etc.)
12. professional information (organisation, title, Board memberships, connections, employment records, etc.)
13. support services (Looked After Children, Support/Key Workers, etc.)
14. safeguarding records (concerns, disclosures, meetings, etc.)
15. identification numbers
16. biometric data

17. financial information
18. information relating to a member's use of their membership and activities at Mahdlo including monitoring and evaluation information either from the young person or in relation to the young person

With regard to visits to our website, Mahdlo may collect the following information:

1. technical information including the internet protocol (IP) address used to connect a computer to the internet
2. user's login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform
3. full Uniform Resource Locators (URL), clickstream to, through and from our website (including date and time), pages viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs), and methods used to browse away from the page

4.2 Mahdlo may also hold special categories of personal data which is considered sensitive personal data and includes information about an individual's race, ethnicity, religion or similar beliefs, trade union membership, health (including physical and mental health), genetic data, biometric data, sexual life and sexual orientation. This sensitive information may be processed not only to meet Mahdlo's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment and to comply with the Equality Act. The processing of DBS (Disclosure and Barring Service) checks is permissible when recruiting for a role which involves working with children or vulnerable adults.

4.3 GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. There are separate safeguards for personal data relating to criminal convictions and offences set out in Article 10. Mahdlo may hold information relating to criminal proceedings or offences or allegations of offences where there is a clear lawful basis to process this data such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk. This processing will be carried out by HR and where appropriate by the Safeguarding Lead.

5.0 Processing of Personal Data

Mahdlo will process personal data lawfully and transparently, providing individuals with an explanation of how and why we process their personal data at the point when the data is collected, as well as when we collect data about them from other sources.

For data to be processed lawfully, at least one of the following legal conditions, as listed in Article 6 of the GDPR, must be met:

1. the processing is necessary for a contract with the data subject;
2. the processing is necessary for Mahdlo to comply with a legal obligation;
3. the processing is necessary to protect someone's life;
4. the processing is necessary for Mahdlo to perform a task in the public interest, and the task has a clear basis in law;
5. the processing is necessary for the legitimate interests pursued by Mahdlo, unless these are overridden by the interests, rights and freedoms of the data subject;
6. if none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

The processing of special categories of personal data is only lawful when the conditions above are met, together with one of the extra conditions set out in Article 9 of the GDPR. These include:

1. the processing is necessary for carrying out Mahdlo's obligations under employment and social security and social protection law;
2. the processing is necessary for safeguarding the vital interests (in emergency situations) of an individual and the data subject is incapable of giving consent;
3. the processing is carried out in the course of Mahdlo's legitimate activities and only relates to individuals we are in regular contact with in connection with our purposes;
4. the processing is necessary for pursuing legal claims;
5. if none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

When personal data is collected directly from an individual we will refer them to Mahdlo's Privacy Policy which explains how their data will be processed, stored and retained. If personal data about an individual is collected from another source, the data subject will be referred to the Privacy Policy and informed (verbally or in writing) about the type and source of the data. Should the data be required to be passed on to another organisation, this information will be provided to the data subject before the data is passed on.

6.0 Consent for Processing Data

6.1 Where none of the legal conditions for processing data apply, and consent is required from the data subject, Mahdlo will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process for which we are requesting consent. Consent can be withdrawn at any time and should this be the case, the processing of the data will stop. Personal data will only be processed for the purposes set out in the Mahdlo's Privacy Policy or for other purposes specifically permitted by law.

6.2 Personal data will only be collected and used for the specific purposes described above and Mahdlo will not collect any more than is required to achieve these purposes.

6.3 Mahdlo will ensure that any personal data held is accurate and, where appropriate, kept up to date. For our workers it is individual's responsibility to ensure that Mahdlo holds the most up to date information regarding your address, emergency contact, and next of kin and banking details. Any information we have about you will not be released to a third party without your express prior permission, unless we have a specific legal requirement to do so.

6.4 Personal data will not be kept longer than is necessary. The data retention guidelines are set out in appendix 1, which cover statutory retention periods, recommended retention periods and retention periods required by Mahdlo's insurers, Ecclesiastical (which take precedence over the GDPR requirements for data retention). The Mahdlo privacy notice for job applicants can be found in appendix 2.

6.5 Mahdlo will ensure appropriate measures are in place to keep personal data secure, including protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

6.6 Mahdlo will keep clear records of our processing activities and of the decisions made concerning personal data.

7.0 Rights of Data Subjects

Mahdlo will process personal data in line with the rights of data subjects, including their right to:

1. request access to any personal data held by us (Subject Access Request);
2. ask to have inaccurate personal data changed;
3. restrict processing, in certain circumstances;
4. object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
5. data portability, that is to receive some or all of their data in a format that can easily be used by another person or organisation;
6. not be subject to automated decisions, in certain circumstances;
7. withdraw consent when we are relying on consent to process their data.

8.0 Direct Marketing

Mahdlo will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulation (PECR) and any laws which may amend or replace the regulations around direct marketing, which means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. The forms of communication include making contact with data subjects by email, text message, social medial messaging, telephone and post.

Contact made by Mahdlo to individuals for the purpose of promoting our aims is defined as marketing, and therefore marketing does not need to be selling anything, or be advertising a commercial product.

Any direct marketing material sent will identify Mahdlo as the sender and will clearly set out how data subjects can object to receiving similar communications in the future. Should an individual object to direct marketing, Mahdlo will stop the direct marketing as soon as possible.

9.0 Subject Access Requests

Individuals have the right to access their personal data and can make a subject access request in writing to HR. They have the right to obtain the following:

1. confirmation that Mahdlo is processing their personal data;
2. a copy of their personal data;
3. other supplementary information which mainly corresponds to the information provided in our Privacy Policy.

Mahdlo will respond to requests without undue delay and act on valid requests within one month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. All data subjects' rights will be free of charge. Mahdlo will follow the ICO guidance on Subject Access Requests (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/)

10.0 Sharing information with other organisations and transferring data

10.1 Mahdlo will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about data sharing through our privacy policy, unless legal exemptions apply to informing data subjects about the sharing. Records will be kept of information shared with a third party.

The Data Protection Act and GDPR does not prevent information sharing in relation to safeguarding. Sharing confidential information without consent will normally be justified as 'in the public interest':

- When there is evidence or reasonable cause to believe that a child is suffering, or is at risk of suffering, significant harm;
- When there is evidence or reasonable cause to believe that an adult is suffering, or is at risk of suffering, serious harm;
- To prevent significant harm to a child or serious harm to an adult, including through the prevention, detection and prosecution of serious crime.

10.2 Data shared for the purposes of reporting e.g. to funders or local partners will be anonymised and be taken from the overall organisational database. Any additional data collected to support monitoring or evaluation for individual projects will be subject to the same data controls described above.

10.3 Supporting partnership working - as a general rule we will only share young people's information to support partnership working (for example with schools, the local authority or Positive Steps) where we have the young person's permission to do so. There may be situations where we have to share information with people outside of Mahdlo in order to protect children and young people's safety, without discussing it with them first, we only do this when we feel they, or another person is likely to come to some harm.

For example:

- Someone they know is being sexually, physically or emotionally abused or threatened with violence.
- Where the life of them or a third party is at risk
- If doing nothing could lead to another person being in a situation of risk, harm or abuse
- Where there may be the need for immediate medical attention including the threat of self harm."

11. Data Processors

Before appointing a contractor who will process personal data on behalf of OnSide (a data processor), due diligence checks will be carried out to check the processor will use appropriate measures to ensure the processing will comply with GDPR.

In the event that Mahdlo is working with agency staff, freelance workers or consultants who require access to the data a contract will be signed requiring that they shall treat all data with the strictest confidence and not divulge or allow to be divulged any personal information held by Mahdlo either during or after the termination of their contract.

12. Data Protection Impact Statements

Should Mahdlo plan to carry out any data processing which is likely to result in a high risk, a Data Protection Impact Assessment will be carried out. Any DPIA will be carried out using the ICO's Code of Practice.

13. Responsibilities

13.1 The responsibility for ensuring organisational practice complies with GDPR lies with the Chief Executive Officer.

The responsibility for ensuring that employee records are processed in line with GDPR lies with HR and for Volunteers/ Mentors with the Training, Volunteer and Quality Standard Manager/ Mentoring Coordinator.

The responsibility for ensuring young people's records are kept secure lies with the Operations Manager with support from HR.

13.2 All workers are responsible and are personally liable for their actions in dealing with personal data and could face prosecution by the Information Commissioner if found to be in breach of the regulations.

13.3 As such Mahdlo requires all employees to comply with GDPR in relation to information about other workers and young people. Failure to do so will very likely be regarded as gross misconduct and dealt with through the disciplinary process.

13.4 Mahdlo has a whistleblowing policy which gives employees rights to report any organisational misconduct without fear of reprisals.

14. Data Storage

14.1 Data will be stored for as long as the data subject has an active relationship with Mahdlo. Some information may need to be retained for a period afterwards to meet statutory and insurance retention requirements (appendix 1).

14.2 Data will be stored in lockable cabinets which only a limited number of staff have access to. Data can only be accessed on a strictly 'need to know' basis. The cabinets are kept in a secure area of the building that the public do not have access to. Those staff who have access to the data have been enhanced DBS checked.

14.3 Electronic versions of the data are kept in restricted access files and a restricted access database. Staff should ensure that when accessing personal data monitors are not left unattended and visible to passers-by. All staff are responsible for logging off when they have finished on the computer to prevent unauthorised access. Passwords for all electronic information are required to be updated monthly.

14.4 Any data communicated by email should be deleted once the matter has been dealt with. Email accounts are password protected.

14.5 Personal data will not be stored on portable devices e.g. memory sticks

14.6 Any printouts, photocopies or other data taken from these electronic records must also be kept secure and destroyed after use.

13. Dealing with Data Protection Breaches

Where individuals think that data may have been breached or lost, this must be reported as soon as possible to Jessica Mistry – HR (jessica.mistry@mahdloyz.org). Breaches of personal data will be recorded, whether or not they are reported to the ICO. Any data breach which is likely to result in a risk to any person will be reported to the ICO within 72 hours of the breach being reported to HR. In addition, where a breach of personal data may cause a high risk to any individual, we will inform data subjects whose information is affected, without undue delay.

Appendix 1: Data Retention Guidelines

Statutory retention Periods

Record	Retention Period	Start of Retention Period	Notes
Health and Safety			
Accident books, accident records/reports	3 year	From date of last entry	If the accident involves a child/young adult, then until that person reaches the age of 21
Medical records as specified by COSHH Regulations	40 years	From date of last entry	
Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates	40 years (medical records) 4 years (medical certificates)	From date of the last entry 4 years from date of issue	
Records of tests and examinations of control systems	5 years	From the date on which the tests were carried out	
Finance			
Accounting records	6 years		For Public Limited Companies
Income tax and NI returns, income tax records & correspondence with HMRC	Not less than 3 years	After the end of the financial year to which records relate	
National minimum wage records	3 years	After the end of the pay reference period following the one the records cover	
HR			
Statutory maternity pay records, calculation, certificates (MAT B1) or other medical evidence	3 years	After the end of the tax year in which the maternity period ends	
Salary records (also overtime, bonuses, expenses)	6 years		
Records relating to working time	2 years	From date on which they were made	
Young People			
Records relating to children and young adults	Until the child/young adult reaches the age of 21		

Recommended (non-statutory) Retention Periods (based on the time limits for potential UK tribunal or civil claims)

Record	Retention Period	Start of Retention Period	Notes
Health and Safety			
Assessments under H&S regulations and records of consultations with safety representatives and committees	Permanently		
HR			
Application forms and interview notes for unsuccessful candidates / CV and cover letters	6 to 12 months		CIPD suggest a year may be more advisable
Inland revenue / HMRC approvals	Permanently		
Money purchase details	6 years	After transfer or value taken	Relates to pension schemes
Pension scheme investment policies	12 years	From the end of any benefit payable under the policy	
Parental leave	5 years	From the end of any benefit payable under the policy From birth/adoption of the child or 18 years if the child receives a disability allowance	
Pensioners' records	12 years	After benefit ceases	
Personnel files and training records (including disciplinary records and working time records)	6 years	After employment ceases	
Redundancy details, calculations of payment, refunds, notification to the Secretary of State	6 years	From the date of redundancy	
Senior executives' records (those on a senior management team)	Permanently	For historical purposes	
Shortlisting notes	6 to 12 months		
Statutory sick pay records, calculations, certificates, self- certificates	6 years	After employment ceases	CIPD recommendation, should there be contractual claims
Trade union agreements	10 years	After ceasing to be effective	

Governance			
Trust deeds and rules	Permanently		
Trustees' minute book	Permanently		

Required Retention Periods as specified by Ecclesiastical (Mahdlo's insurers)

As incidents of abuse may only come to light after a long period of time, the long-term availability of relevant documents and related correspondence is of crucial important should allegations of abuse arise. In order to assist in the handling and defence of claims for abuse and to demonstrate that Mahdlo is compliant with Ecclesiastical's Risk Management Condition, Ecclesiastical requires secure retention of all relevant personnel employment (employees & volunteers) and training records, safeguarding policies and other abuse-incident-related correspondence. Due to the potential for long latency periods, Ecclesiastical require such records to be kept for no less than 50 years.

Record	Retention period	Notes
Application forms, all correspondence relevant to the applications including any correspondence in relation to gaps in employment	50 years	
Records that Mahdlo has obtained suitable references and details of any follow up enquiries carried out	50 years	Does not need to be a copy of the actual reference
Records that Mahdlo has carried out a suitable check to verify the identity of the applicant including the nature of the check	50 years	Does not need to be copies of passports/drivers licences/etc.
DBS or similar statutory disclosures i.e. DBS certificate reference number and any relevant follow up correspondence for all employees and volunteers for which they are obtained under the recruitment policy	50 years	In accordance with DBS Code of Practice, NOT a copy of the actual certificate
Safeguarding Policy including copies of previous versions; full details of all training delivered in relation to the policy including details of who attended and dates attended	50 years	
Records of abuse allegations or incidents and action taken including notifications to the appropriate authorities: • Record of all know abuse allegations and incidents • Details of the outcome of any investigation & any follow-up action taken by Mahdlo • Details of any notification made to relevant authorities; this could include Police, DBS and local safeguarding boards	50 years	

Copies of relevant information and accompanying correspondence relating to abuse, assault or molestation of or by Mahdlo's service users whilst in our care, contained in their referral assessment treatment and care plans	50 years	
Cause for concern forms and other paperwork required under Mahdlo's Safeguarding Policy	50 years	

Appendix 2: Mahdlo's Applicant Privacy Notice

Mahdlo (Oldham Youth Zone)

As part of any recruitment process, Mahdlo collects and processes personal data relating to job applicants. Mahdlo is committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

What information do we collect?

Mahdlo collects a range of information about you. This includes:

- Your personal details e.g. name, address and contact details, including email address and telephone number where this has been supplied on your Application form/CV/Cover Letter
- Details of your qualifications, skills, experience and employment and training history;
- Information about your current level of remuneration, including benefit entitlements; where this has been supplied on your Application form/CV/Cover Letter
- Whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; where this has been supplied on your Application form/CV/Cover Letter
- Information about your entitlement to work in the UK; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief – where this has been supplied

Mahdlo collects this information in a variety of ways. For example, data might be contained in application forms, CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, online or face to face.

Mahdlo will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from Disclosure and Barring Service checks. Mahdlo will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does Mahdlo process personal data?

Mahdlo needs to process data to take steps at your request prior to entering into a contract with you. We also need to process your data to enter into a contract with you. In some cases, Mahdlo needs to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

Mahdlo has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Mahdlo may also need to process data from job applicants to respond to and defend against legal claims.

Mahdlo processes health information only if we need to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

Where Mahdlo processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes, but only with the consent of job applicants, which can be withdrawn at any time. For some roles, we are obliged to seek information about criminal convictions and offences. Where this is the case, we do so because it is necessary for it to carry out our obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, Mahdlo do not habitually keep personal data on file in case there are future employment opportunities for which you may be suited. Nevertheless, if it is so required, Mahdlo

will ask for your consent before we keep your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

Mahdlo will not share your data with third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, and the Disclosure and Barring Service to obtain necessary criminal records checks. Mahdlo will not transfer your data outside the European Economic Area.

How does Mahdlo protect data?

Mahdlo takes the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties, and is stored in a confidential electronic format, or locked physical storage with limited access.

For how long does Mahdlo keep data?

If your application for employment is unsuccessful, Mahdlo will hold your data on file for 12 months after the end of the relevant recruitment process. If you request or agree to allow Mahdlo to keep your personal data on file, we will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period, or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in an organisational privacy notice.

Your Rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require Mahdlo to change incorrect or incomplete data;
- require Mahdlo to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where Mahdlo is relying on its legitimate interests as the legal ground for processing; and
- ask Mahdlo to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Mahdlo's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact HR at HR@mahdloyz.org

If you believe that Mahdlo has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to Mahdlo during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all. You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.