

Data Protection Policy

For the purposes of this policy the Company or us refers to Midlothian Sure Start, the Data Subject refers to you, the reader.

Data Protection

The security and privacy of your data is taken seriously by us, but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We are committed to complying with all our Data Protection legal obligations.

This policy applies to current and former employees, workers, volunteers, interns, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from the person responsible for Data in the Company.

The Company has taken steps to protect the security of your data in accordance with our Data Protection Policy and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time.

Data Protection Principles

Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

The types of personal data we collect and use about you is included in the Privacy Notice that is issued with your contract of employment.

How we define special categories of personal data

'Special categories of personal data' are types of personal data consisting of information as to:

- Your racial or ethnic origin;
- Your political opinions;
- Your religious or philosophical beliefs;
- Your trade union membership;
- Your genetic or biometric data;
- Your health;
- Your sexual preferences, sex life and/or sexual orientation; and
- Any criminal convictions and offences.

We may hold and use any of these special categories of your personal data, as detailed in the Privacy Notice, in accordance with the law.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage;
- Adaption or alteration;
- Retrieval, consultation or use;
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination; and
- Restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data

The Company will process your personal data (including special categories of personal data). We will use your personal data for:

- Performing the contract of employment (or services) between us;
- Complying with any legal obligation; or
- If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Examples of when we might process your personal data can be found in the Employee Privacy Notice (Appendix 1). We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the person responsible for Data in the Company.

We do not need your consent to process **special categories** of your personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- Where you have made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes stated in the Privacy Notice, in particular, we may use information in relation to:

- Your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- Your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- Your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

Sharing your personal data

Sometimes we might share your personal data with group companies or our business partners, contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We use the following contractors to carry out our Company business:

- Payroll/accountant to store and manage your personal data with regard to your pay and Partner Funders
- Pension Advisor to advise and support your pension contributions to pension provider
- Outsourced HR company
- IT consultants and database managers/companies on retainer and on an adhoc basis

We do not send your personal data outside the European Economic Area under the General Data Protection Regulation. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for the Company

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's IT Security and Data Retention policies.

The Business Support Manager is responsible for reviewing this policy on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person and address any written requests to them.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of The Business Support Manager.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager or of the Business Support Manager.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from the Business Support Manager who is responsible for Data in your Company if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Business Support Manager immediately and keep any evidence you have in relation to the breach.

Subject Access request

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to The Business Support Manager who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to The Business Support Manager who is responsible for Data in the Company. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.
- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do so you should contact the person responsible for Data in the Company.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the person for responsible for Data in the Company.
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the person for responsible for Data in the Company.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the person for responsible for Data in the Company.
- You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Retention of records

Midlothian Sure Start follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code and as advised by legislation of funding requirements. In certain circumstances a specific business case will support a longer period. Our retention schedule can be found in our Retention Policy and Schedule.

See also:

Privacy Statements- staff and general

Date of 1 st Issue	Revision	Agreed	Status	Responsibility	Review Date
5 th May 2021	4	5 th June 2021	Approved	HR Committee	June 2024

EMPLOYEE PRIVACY NOTICE

Appendix I

Midlothian Sure Start is committed to protecting the privacy and security of your personal information and we will always treat you and your data with the respect you deserve.

This Privacy Notice covers how we collect, use, store and disclose the data that you supply to us and your rights about data that we hold about you. It applies to current and former employees, workers, volunteers, interns and contractors and does not form part of any contract of employment or other contract to provide services. For more information please contact Claire Young who will provide you with our Data Protection Policy.

THE INFORMATION WE COLLECT FROM YOU

Personal individual information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We will collect, store, and use the following categories of personal information about you:

PC - Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

DOB - Date of birth.

G - Gender.

MSD - Marital status and dependants.

NOK - Next of kin and emergency contact information.

NI - National Insurance number.

FI - Bank account details, payroll records, travel logs and expenses and tax status information.

EB - Salary, annual leave, pension and benefits information.

SD - Start date.

WL - Location of employment or workplace.

RI - Recruitment information (including copies of right to work documentation, passport, references and other information included in a CV or cover letter or as part of the application process).

ER - Employment records (including job titles, work history, working hours, training records and professional memberships).

COM - Compensation history.

PER - Performance information.

DG - Disciplinary and grievance information.

CCTV - CCTV footage and other information obtained through electronic means such as swipe card records.

ICS - Information about your use of our information and communications systems.

P - Photographs.

We may also collect, store and use “special categories” of more sensitive personal data which require a higher level of protection:

HR - Information about your health, including any medical condition, health and sickness records (including Occupational Health records).

A - Absence notes.

ED - Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.

TU - Trade union membership.

GI - Genetic information and biometric data.

CC - Information about criminal convictions and offences.

How the information is collected

We collect personal information through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers or other background check agencies [credit reference agencies, PVG/Police Checks]. We may collect additional personal information in the course of job-related activities throughout the period of you working for us.

When we will use your personal information

We need all the categories of information identified above primarily to allow us to perform our contract with you[*] and to enable us to comply with legal obligations[**]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties[***] (provided your interests and fundamental rights do not override those interests). We will process your personal information as follows, the asterisks show the purpose for processing:

Purpose	Type of data	Lawful basis
Making a decision about your recruitment or appointment.	PC, RI, ER	***
Determining the terms on which you work for us.	EB, SD, PC, RI, ER	***
Checking you are legally entitled to work in the UK.	PC, DOB, NI	**
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	PC, NI, FI, SD	** *
Providing the following benefits to you: Employee Assistance Programme (Health Assured)	PC, DOB, G, MSD, NOK, NI, FI, EB, SD	*
Liaising with your pension provider.	PC, DOB, NI, EB, SD	*
Administering the contract we have entered into with you.	PC, NOK, NI, FI, EB, SD, WL, PER, DG, ED	*** *
Business management and planning, including accounting and auditing.	PC, DOB, G, NI, FI, EB, SD, WL, PER, DG, ICS, HR, ED, TU	***

Conducting performance reviews, managing performance and determining performance requirements.	PC, EB, SD, WL, PER, DG, CCTV, ICS, ED	*** *
Making decisions about salary reviews and compensation.	PC, FI, EB, SD, WL, RI, ER, PER, DG, CCTV, ICS	*** *
Assessing qualifications for a particular job or task, including decisions about promotions.	PC, RI, ER, PER, DG, ED	*** *
Gathering evidence for possible grievance or disciplinary hearings.	PC, PER, DG, CCTV, ICS, ED	*** *
Making decisions about your continued employment or engagement.	PC, PER, DG, CCTV, ICS, ED	
Making arrangements for the termination of our working relationship.	PC, NI, FI, EB, PER, DG, ED	*** *
Education, training and development requirements.	PC, ER, PER, DG, ED	*** *
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	PC, FI, EB, COM, PER, DG, CCTV, ICS, P, HR, A, ED, GI	***
Ascertaining your fitness to work and managing sickness absence.	PC, DOB, G, MSD, NOK, WL, PER, DG, CCTV, ICS, P, HR, ED	*** *
Complying with health and safety obligations.	PC, NOK, WL, ED	** *
To prevent fraud.	PC, NI, FI, RI, ER, GI	***
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	PC, CCTV, ICS	***
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	PC, CCTV, ICS	***
To conduct data analytics studies to review and better understand employee retention and attrition rates.	PC, DOB, G, MSD, HR, ED	***
Equal opportunities monitoring.	PC, DOB, G, MSD, HR, ED	***

Please refer to our Data Protection Policy.

Failure to provide information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing employee benefits), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

SENSITIVE PERSONAL INFORMATION

“Special categories” of particularly sensitive personal information require higher levels of protection. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our Data Protection Policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our Data Protection Policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions and access your DBS portal.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current, so please let us know if your information changes.

DISCLOSURE/DATA SHARING

We may have to share your data with third parties, including third-party service providers (including contractors and designated agents); other entities in the group; in the context of a sale of the business; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks legal disputes. The following activities are carried out by third-party service providers: HR Services, Pension administration, Account auditors and Partner Funders.

We do this where required by law; where it is necessary to administer the working relationship with you; or where we have another legitimate interest in doing so.

We require third parties to respect the security of your data and to treat it in accordance with the law.

DATA RETENTION

We must store most of your HR data for a period of at least 6 years following the termination of your employment; some personal financial data will be destroyed after 2 years; Health and Safety information must be held for a minimum of 40 years.

YOUR RIGHTS

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. Please refer to our DSAR Procedure for more information.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Please contact the Business Support Manager who is responsible for Data Protection in our Company.

COMPLAINTS & QUESTIONS

If you have any questions about this privacy notice or how we handle your personal information, please contact the Business Support Manager who is responsible for Data Protection in our Company. If we have breached our duty of care, we will take appropriate action.

If you are not satisfied by our response you also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (**Email:** casework@ico.org.uk)

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.