Steps Data Protection Policy

Steps is committed to protecting the rights and freedoms of data subjects and safely and securely processing people's personal data in accordance with all our legal obligations

Steps
Conductive Education Centre

Registered Charity Number: 1063143

Date policy passed by Trustees: Oct 2019

Introduction

Steps is committed to protecting the rights and freedoms of data subjects and safely and securely processing people's personal data in accordance with all our legal obligations. We hold personal data about our trustees, members, employers, volunteers, partners, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure you understand the rules governing the use of personal data, which you have access to during your work with Steps.

Definitions

Business purposes

- The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and
- good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

Personal data

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data we gather may include individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.

Special categories of personal data

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data Controller

‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

‘Processor’ means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of a data controller.

Processing ‘Processing’ means any action which is performed on/with personal data, by manual or automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Supervisory Authority

This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office

Scope

This policy applies to all trustees and employees and you should ensure that you are familiar with this policy and comply with its terms. This policy supplements other policies set out in our Employee Handbook. We may supplement or amend this policy from time to time. Any new or modified policy will be circulated to you before being adopted.

The Steps Board of Trustees retains overall responsibility for this policy. As our data protection lead, the Chair of Trustees has overall responsibility for the day-to-day implementation of this policy.

Data Protection Principles

We shall comply with the principles of data protection (the principles) as set out in the EU general Data Protection Regulation. (We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. Lawful, fair and transparent - Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose - Data can only be collected for a specific purpose.

3. Data minimisation - Any data collected must be necessary and not excessive for its purpose.

4. Accurate - The data we hold must be accurate and kept up to date.

5. Retention - We cannot store data longer than necessary.

6. Integrity and confidentiality - The data we hold must be kept safe and secure.

Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle.

You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Data Protection Principles. This must be kept up to date and saved on our shared data protection folder.

To comply with data protection laws and the accountability and transparency principle of GDPR, we must demonstrate compliance. You are responsible for ensuring you understand your responsibilities to ensure we meet the following data protection obligations:

a. Put in place and fully implement appropriate policies and procedures when processing personal data.

b. Maintain up to date and relevant documentation on all processing activities

c. Conducting Data Protection Impact Assessments (where necessary)

d. Implement measures to ensure privacy by design and default, including:
• Data minimisation
• Transparency
• Allowing individuals to monitor processing
• Creating and improving security and enhanced privacy procedures on an ongoing basis

Fair and Lawful Processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. If we do not have consent and cannot apply another lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. It is your responsibility to check the lawful basis for any data you are working with and ensure all your actions comply with the lawful basis applied. Data subjects have the right to have any data unlawfully processed erased. At least one lawful basis from this list must apply whenever we process personal data:

1. Consent - We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. Contract - The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal Obligation - We have a legal obligation to process the data (excluding a contract).

4. Vital Interests - Processing the data is necessary to protect a person's life or in a medical situation.

5. Public Function - Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Legitimate Interest - The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Before deciding on a lawful basis, you must first establish that the data processing you plan to undertake is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose of your activity. You cannot rely on a lawful basis if you can reasonable achieve the same purpose by some other means other than processing personal Remember that more than one basis may apply, and you should rely on what is most appropriate to the purpose, not what is easiest, quickest or cheapest.

Consider the following factors and document your answers:

a. What is the purpose for processing the data?

b. Can you reasonably achieve this purpose in another way?

c. Is there a choice as to whether to process the data?

d. Who does the processing benefit?

e. Is this likely to be the same lawful basis that the data subject would expect us to apply?

f. What is the impact of the processing on the individual?

g. Are you in a position of power over the individual?

h. Are they a vulnerable person?

i. Would they be likely to object to the processing?

j. Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Controlling and Processing Data

We are classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office to continue lawfully controlling and processing data.

When acting as a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

• Not use a sub-processor without written authorisation of the data controller

• Co-operate fully with the ICO or other supervisory authority

• Ensure the security of the processing

• Keep accurate records of processing activities

• Notify the controller of any personal data breaches

Special Categories of Personal Data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:
• Race
• Ethnic origin
• Politics
• Religion
• Trade union membership
• Genetics
• Biometrics (where used for ID purposes)
• Health
• Sexual orientation

In most cases where we process special categories of 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.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Our Responsibilities

a. Analysing and documenting the type of personal data we hold

b. Setting and regularly reviewing data protection policies and procedures

c. Ensuring all data processing procedures are lawful and meet required standards

d. Implementing and reviewing procedures to detect, report and investigate personal data breaches

e. Storing data in safe and secure ways and ensuring all systems, services, software and equipment meet acceptable security standards.

f. Assessing the risk that could be posed to individual rights and freedoms should data be compromised

g. Researching and approving third-party providers, such as cloud services we are considering using to store or process personal data on our behalf and ensuring appropriate contracts are in place.

h. Providing appropriate guidance and training for those working within this policy

i. Answering questions on data protection from staff, board members and other stakeholders

j. Responding to individuals such as clients and employees who wish to know which data is being held on them by us.

Your Responsibilities

a. Fully understand your data protection obligations

b. Check that any data processing activities you are dealing with comply with our policy and are justified

c. Do not use data in any unlawful way

d. Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions

e. Comply with this policy at all times

f. Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

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 to happen.

Individuals may ask that we correct inaccurate personal data relating to them.

Data Security

We will keep all personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

a. We will store personal data on secure and backed up electronic and cloud-based systems which are approved and monitored by Steps

b. Personal data stored electronically will be protected by strong passwords that are changed regularly.

c. In limited cases when personal data is stored on removable media (e.g. CDs or USB sticks) these will be encrypted, or password protected and locked away securely when not being used.

d. In limited cases when personal data is stored on printed paper, it will be kept in a secure place where unauthorised people cannot access it and shredded as soon as it is no longer needed

e. Steps must approve any cloud service used to store data

f. All personal data will be regularly backed up.

g. Personal data will never be saved directly to mobile devices such as laptops, tablets or smartphones

h. All computers and servers containing sensitive data will be approved and protected by security software

i. All possible technical measures will be put in place to keep data secure

Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, and consistent with our agreed data retention guidelines.

Transferring Data Internationally

Our operations are based solely in the UK and we will store all personal data within the European Economic Area.

Rights of Individuals

Individuals have rights to their personal data, which we will respect and comply with to the best of our ability.

We will ensure individuals can exercise their rights in the following ways:

Right to be informed

- Providing a privacy notice which is concise, transparent, easily accessible (free of charge) and written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

Right to rectification

Rectifying or amending the personal data of an individual if requested or we are notified that it is inaccurate or incomplete (this will be done without delay and within no more than one month).

Right to erasure

Deleting or removing an individual's data if requested and there is no compelling reason or legal obligation for its continued processing.

Right to restrict processing

Complying with requests to restrict, block, or otherwise suppress the processing of personal data. (We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.)

Right to data portability

- Providing individuals with their data if requested so that they can reuse it for their own purposes or across different services.
- Providing data in a commonly used, machine-readable format, and sending it directly to another controller if requested by the data subject.

Right to object

- Respecting the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- Respecting the right of an individual to object to direct marketing, including profiling.
- Respecting the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling

- Respecting the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy Notices

We will adopt and publish a clear and concise Privacy Notice. The notice will explain how and why we use personal data and ensure individuals remain informed and in control of the information we hold. A copy of or link to our Privacy Notice will be supplied at the time any personal data is obtained directly from an individual (data subject).

If the data is not obtained directly from the data subject, the Privacy Notice will be provided within a month of us obtaining the data. If the data is being used to communicate with the individual, then the notice must be supplied at the latest when the first communication takes place.

If disclosure of the data to a third party is envisaged, then the Privacy Notice will be supplied prior to the data being disclosed.

What our Privacy Notice Includes

Our Privacy Notice will be concise, transparent, intelligible and easily accessible. It will be provided free of charge and written in clear and plain language.

As a minimum the following information will be included in our Privacy Notice:

- Our identity and contact information as the data controller
- What personal data we collect and process and the source of the personal data
- (including whether it came from publicly available sources).
- The purpose(s) for which we collect the data and the lawful basis for doing so
- How we process and protect personal data
- Individuals rights with regards to the personal data we collect
- How we disclose or share data and the categories of recipients of the personal data

- Detailed information of any transfers to third countries and safeguards in place
- The criteria used to determine the retention period and details of data disposal
- The right to lodge a complaint with the ICO, and internal complaint procedures
- Any existence of automated decision making, including profiling and information about
- how those decisions are made.

Subject Access Requests

An individual has the right to request confirmation from us that their data is being processed, access to their personal data we hold and to supplementary information which will be provided in our privacy notice. We will provide an individual with a copy of the information they request, free of charge. This will be sent without delay and within a maximum of one month. We will try to provide individuals with access to their information in commonly used electronic formats (PDF) and where possible, provide direct access to the information through a secure cloud-based system.

We can refuse to respond to certain requests, and can, in circumstances of the request being unfounded or excessive, charge a reasonable fee to cover our costs in dealing with the request.

Once a subject access request has been made, we will not change or amend any of the data that has been requested. Doing so is a criminal offence.

Erasing Personal Data

We operate a data minimisation policy and will routinely delete or destroy personal data we hold as appropriate and in line with our data retention guidelines. Data we find to be inaccurate and that cannot be updated will also be erased.

Individuals have a right to have their data erased and for processing to cease at any time 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 overriding legitimate interest
- for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

- We will erase all personal data as requested by an individual without delay and within one month.
- We will 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 public health purposes in the public interest
- For archiving purposes in the public interest or for scientific, historical or statistical research
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those third-party recipients.

Third Parties

Using third party controllers and processors

As a data controller and/or data processor, we will have written contracts in place with any third-party data controllers or data processors that we engage. The contract will contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts will comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and data processors will set out:

a. The subject matter and duration of the processing

b. The nature and stated purpose of the processing activities

c. The types of personal data and categories of data subject

d. The obligations and rights of the controller.

As a minimum our contracts will include the following terms:

- The processor must only act on the written instructions of the controller (unless required by law to act without such instructions)
- The processor must ensure that people processing the data are subject to a duty of confidence
- The processor must take appropriate measures to ensure the security of processing
- The processor must only engage a sub-processor with the prior consent of the data controller and a written contract
- The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- The processor must delete or return all personal data to the controller as requested at the end of the contract
- The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Criminal Offence Data

Any criminal record or DBS checks we complete will be justified by law and cannot be undertaken based solely on the consent of the subject. We will not keep a comprehensive register of criminal offence data. All data relating to criminal offences is a special category of personal data and will be treated as such.

Data audits - We will undertake regular data audits to ensure we understand what data we hold, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Training - We will ensure everyone receives adequate information, guidance or training on provisions of data protection law specific and relevant to their role with us. You must complete all mandatory

training as requested. If your role or responsibilities change you are responsible for requesting new data protection training as appropriate.

Reporting Breaches

Any breach of this policy or of data protection laws must be reported to the Executive Director as soon as practically possible (this means as soon as you have become aware of a breach). We have a legal obligation to report certain data breaches to the ICO within a maximum of 72 hours.

By reporting a breach quickly and openly you will enable us to:

- Investigate the breach and take remedial steps if necessary
- Maintain an accurate register of policy and data breaches
- Notify the ICO as appropriate/required

We take compliance with this policy very seriously as failure to comply puts you and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our normal disciplinary procedures.

If you have any questions or concerns about this policy, please contact the Chair of Trustees.

Policy updated October 2019

Signature of Trustee: Date: 24th October 2019