



Safeguarding and Protecting People from Harm Policy and Procedure

Document Owner:	CEO & Trustee Board
Designated Lead	Leigh Bowman-Perks leigh@inspiringleadership-int.com T: +44 (0) 3336 888444
Trustee with designated oversight :	Nicola Kerr-Shaw
Governance:	Level 1: Victoria Cope - Audit and Risk Assurance Committee Chair Trustee Board Level 2: Trusteed Board
Date Approved by Management:	1st April 2020
Next Review Date by Trustees:	16 June 2022 TBC



Data Protection and GDPR Policy

Contents

Data Protection and GDPR Policy	3
About Inspiring Leadership Trust.....	4
Policy Statement	4
About This Policy.....	4
Complaints	4
Disciplinary Consequences.....	5
Changes to this Policy	5
Definitions	5
Data controller	5
Data processor	5
Data subject	5
Data Protection Officer	5
Personal Data	5
Sensitive Data.....	6
Data Protection Principles	6
Fair and Lawful Processing.....	6
Processing for Limited Purposes	6
Adequacy, Relevance and Limitation of Processing	7
Accuracy of Data	7
Timely Processing.....	7
Processing in line with Data Subjects' Rights.....	7
Notifying Data Subjects.....	7
Children's Data:.....	8
Making a Data Access Request	8
Handling of Data Access Requests	8

Data Security	9
Security Procedures	9
Methods of Disposal	10
Collection, Disclosure and Sharing of Personal Data	10
Transferring Personal Data Outside of the EEA.	10
Appendix 1: Schedule of Data Processing Activities	12
Appendix 2: Relevant Contacts	13

About Inspiring Leadership Trust

The Inspiring Leadership Trust offers a wide range of information and advice services to young women, families, and businesses. We campaign to inspire and empower vulnerable women and their families to achieve their full potential. Through mobilising leadership networks, charitable collaborations and scalable projects, our mission is to empower women and girls to achieve financial and personal independence through education and employment opportunities.

Policy Statement

In the course of our normal work, the Inspiring Leadership Trust receives, uses and stores personal information about our employees, volunteers, customers, facilitators, agency and contract workers as well as users of our services. It is essential that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (collectively referred to as the Data Protection Requirements). The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

We take our data protection duties seriously and commit to respecting the trust that is placed in us to store, use and process personal information appropriately and responsibly.

About This Policy

This policy, and any other documents referenced in this policy, set out the basis on which we will process any personal data we collect. This policy does not form part of any employee's contract of employment or volunteer agreement and may be amended at any time. However this policy applies to anyone who works with Inspiring Leadership Trust (including trustees, agency workers and volunteers) and who might have access to sensitive or personal data.

The Data Protection Officer is responsible for ensuring compliance with the Data Protection Requirements and this policy. Any questions about the operation of this policy or concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer or reported in line with Inspiring Leadership Trust's Whistleblowing Policy or Grievance Policy.

See [Appendix 2](#) for current contact details of the Data Protection Officer.

Complaints

Should you wish to register a complaint we will ask for your name, contact details and details about the complaint. This data is essential to enable us to respond to your complaint as well as to monitor and improve our organisation.

This data will be shared with any parts of the Inspiring Leadership Trust or any third parties who are involved in the complaint or required to resolve the complaint, for example, agencies with whom we have partnered.

Disciplinary Consequences

Employees and volunteers who do not adhere to this policy will face disciplinary and, if appropriate, legal action.

The Inspiring Leadership Trust will investigate every breach of this policy. The Trust will terminate the employment of anyone who wilfully or regularly breaches this policy. The Trust reserves the right to punish as it sees fit, any unintentional breach of this policy depending on the frequency and severity of the breach

This policy is binding even after separation of employment.

Changes to this Policy

We reserve the right to change this policy at any time. If we make any changes in the way we use personal information we will make this clear on the Inspiring Leadership Trust website or by contacting data subjects directly.

Definitions

Data controller

The person or people responsible for determining the purposes and means of collecting personal data.

Data processor

The person or people responsible for processing personal data on behalf of a data controller. Processing is any activity that involves personal data including: obtaining, recording, holding, organising, amending, retrieving, using, disclosing, erasing or destroying data. Processing also includes transferring personal data to third parties.

Data subject

The person to whom personal data or sensitive data relates. Each of us is a data subject of our own personal data and sensitive data. We own that data and usually have the right to determine how and when it is used, stored, disclosed to third parties and erased.

Data Protection Officer

The person charged with ensuring that data is handled responsibly, including monitoring compliance with the Data Protection Act 2018 and GDPR. The Data Protection Officer is also responsible for educating and training anyone within the organisation who handles personal data about the processes and procedures we use to maintain the security of that data.

Personal Data

Personal data means any data relating to a living person which can be used to identify that person directly or indirectly from that data alone, or from that data in combination with other information in our possession. Personal data can be stored electronically or physically and can include, but is not limited to, the data subject's name, phone number, address, job title, email address, IP address, their phone's IMEI number, National Insurance number, passport number, etc.. Where the ability to identify a data subject depends partly on the data we hold and partly on other information (not

necessarily present in the data), the data we hold is still considered personal data, for example if a unique reference number is attached to a data set.

Personal data also includes any expressions of opinion about the data subject and any information about the intentions of the data controller or any other person toward the data subject.

Sensitive Data

Sensitive data is a specific set of data types which must be treated with extra security. Sensitive data is information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions.

We take greater care when we handle sensitive data because it could be used to discriminate against the data subject. Sensitive data is only processed under strict conditions and with the consent of the data subject.

Data Protection Principles

Anyone processing personal data, must ensure that data is:

- a. collected for specified, explicit and legitimate purposes and processed for a compatible purpose.
- b. processed fairly, lawfully and in a transparent manner.
- c. adequate, relevant and limited to only what is necessary for the intended purposes.
- d. accurate, and where necessary, kept up to date.
- e. kept in a form which permits identification for no longer than necessary for the intended purposes.
- f. processed in line with the data subject's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- g. not transferred to people or organisations situated in countries without adequate protection.
- h. not transferred to other people or organisations without the data subject's knowledge and, if applicable, consent.

Fair and Lawful Processing

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose and when the data subject has given their consent. Such lawful purposes include (but are not limited to): the processing necessary for performing a contract with the data subject, for compliance with a legal obligation, or for the legitimate interest of the business. When we process sensitive data, we will meet the relevant additional conditions.

Processing for Limited Purposes

In the course of our business, we might collect and process the personal data set out in Schedule 1 (see [Appendix 1](#)). This might include data we receive directly from a data subject (for example, when they complete forms or correspond with us by post, phone, email etc.) and data we receive from other sources (for example, business partners, technical sub-contractors, payment and delivery services etc.). We will only process personal data for the specific purposes set out in Schedule 1 or

for any other purposes specifically permitted by the Data Protection Requirements. We will state those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Adequacy, Relevance and Limitation of Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accuracy of Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy or erase from our systems all data which is no longer required.

Processing in line with Data Subjects' Rights

We will process all personal data in line with data subjects' rights, in particular their rights to:

- a. know that their personal data is being processed.
- b. request access to any data we hold about them (see also [Subject Access Requests](#)).
- c. request rectification, erasure or restriction on processing of their personal data.
- d. lodge a complaint with a supervisory authority.
- e. obtain and reuse their personal data for their own purposes across different services (this right is known as the right to data portability).
- f. object to the processing of their data, including for direct marketing.
- g. not be subject to automated decision making, including profiling, in certain circumstances.

Notifying Data Subjects

If we collect personal data directly from a data subject, we will tell them:

- a. that we are the data controller with regard to that data.
- b. that they can contact us via info@inspiringleadershiptrust.com.
- c. the name and contact details of the Data Protection Compliance Manager and Data Protection Office (see [Appendix 2](#) for current details).
- d. the purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
- e. where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
- f. the types of third parties, if any, with which we will share or disclose that personal data.
- g. whether we will transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place in that situation.
- h. how long we will store their data or the criteria used to determine that duration.
- i. that they have the right to request access to, correction of and erasure of the personal data we store about them, as well as the right to limit how we process their data.
- j. how data subjects can limit our use and disclosure of their personal data.
- k. that they have the right to object to us processing their data.
- l. that they have the right to data portability and what that means.

- m. that they have the right to withdraw their consent for us to process their data at any time (if consent was given), and that this right does not affecting the lawfulness of us processing their data before the consent was withdrawn.
- n. that they have the right to lodge a complaint with the Information Commissioners Office.
- o. the source of their data if we gathered their personal data from external sources, including publicly accessible sources.
- p. whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.
- q. whether they are obliged to provide the personal data and any consequences of failure to provide their data.
- r. whether we use any automated decision-making, including profiling, in relation to their data. If we do, we will also give meaningful information about the logic involved and the significance and the envisaged consequences of that decision making for the data subject.
- s. know if we received their data from other sources. If we do, we will also tell them about the categories of personal data we received. We will provide the data subject with this information as soon as possible and at the latest within one month.

Children's Data

Although children under 16 can fundraise with the consent and support of a guardian, we do not record their contact information. Instead, their parent or guardian's details are recorded along with the parent or guardian's contact preferences. If we store personal data relating to young people over the age of 16, we will still require a guardian as reference (for school contacts this can be a teacher).

Where a user of our service is under the age of 16, our service is always provided with the family, parent or carer. Data is supplied to us where we have a legal basis to collect and retain that data as per the contracts, or included in the case notes provided, for example by paediatricians. This information is not shared with anyone who is not connected to providing the service.

Making a Data Access Request

As a data subject, you can make a formal request to receive a copy of the personal data we hold about you at any time. You can also request that we update, correct or delete the data we hold about you. To make these requests, write to us at:

- info@inspiringleadershiptrust.com
- or 53 London House, 172 Aldersgate Street, London EC1A 4HU

You can also request changes to the ways we contact you by writing to us or by calling us on 07591 205891.

Handling of Data Access Requests

Employees who receive data access requests will forward them to the Data Protection Officer (See [Appendix 2](#)) as soon as possible.

When we receive an enquiry relating to data protection by telephone, we will always suggest that the caller puts their request in writing. We will only disclose personal data we hold on our systems to a telephone caller if we are able to check the caller's identity to make sure that they are entitled to receive that data.

Where a request is made electronically, data will be provided electronically where possible. Our employees will refer such requests to their line manager or the Data Protection Officer (see

[Appendix 2](#)) for assistance when it is not clear that the conditions set out in this policy have been or can be met.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

We will maintain data security by protecting the confidentiality, integrity and availability of data subjects' personal data. Confidentiality means that only people who are authorised to use the data can access it. Integrity means that personal data must be accurate and suitable for the purpose for which it is processed. Availability means that authorised users can access the data if they need it for authorised purposes.

We will maintain the confidentiality, integrity and availability of data subjects' data as follows:

- a. Personal data will be stored on the Inspiring Leadership Trust's central computer system, not on individual PCs.
- b. Staff will ensure that computer screens do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- c. Putting in place adequate security procedures. See [Security Procedures](#).
- d. Disposing of data appropriately. See [Methods of Disposal](#).

Security Procedures

We do not have our own premises. When we are offsite, premises are entry controlled. Any stranger seen in entry-controlled areas will be reported to reception / site owners/ the client and also to a member of ILT staff.

Everyone who works with us is required:

- a. to sign a non-compete and/or non-discloser agreement.
- b. to maintain strong passwords when using digital devices and adhere to our password policy
- c. to view personal or sensitive data only on secured devices.
- d. to view only the data to which they have legitimately been granted access by an administrator on the authorisation of senior management of Inspiring Leadership Trust.
- e. to disclose personal information to others who work with us only when it is necessary, authorized and in accordance with this policy.
- f. never to disclose personal information to anyone outside of Inspiring Leadership Trust, unless it is done so in accordance with this policy.
- g. never to reproduce documents or files containing personal or sensitive data, nor to store those documents or files on an insecure device.
- h. never to use confidential information for any personal benefit or profit.
- i. to return any documents or files containing personal or sensitive data to us and delete them from their personal devices when they stop working with us.

We provide staff with secure lockable desks and cupboards. Desks, filing cabinets and cupboards are kept locked if they hold confidential information of any kind. Personal information is always considered confidential.

We practice data minimisation. Data minimisation is limiting the personal data collected and processed to include only information that is relevant or necessary to the purposes of the data collection.

We also practice encryption and pseudonymisation of data. Pseudonymisation is the replacement or removal of data which could be used to identify the data subject.

Methods of Disposal

Paper documents are shredded when they reach the end of their retention period. Digital storage devices are physically destroyed when they are no longer required.

Collection, Disclosure and Sharing of Personal Data

We use third-party organisations such as JustGiving and Virgin Money Giving to help us collect donations.

In general, we do not share personal data with other organisations. However we might share personal data we hold:

- a. with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- b. if we are required to do so for legal or regulatory reasons.
- c. with a regulatory body if it is requested as part of an investigation or audit.
- d. to respond to and deal with a complaint.
- e. to administer a Gift in Will.
- f. to fulfil our marketing.
- g. if we examine a venture or partnership that requires disclosing some information, within legal boundaries and in accordance with this policy.

In these cases, the employees and volunteers involved will obtain all necessary authorisations and document their disclosure procedure.

Personal data will only be transferred to another party if they agree to comply with Data Protection Requirements and if they put in place adequate measures to maintain the security of that data.

Transferring Personal Data Outside of the EEA.

Data we hold is hosted on servers located in the UK. These servers will not be transferred out of the European Economic Area (EEA).

We might transfer any personal data we hold to a country outside the EEA or to an international organisation, provided that one of the following conditions applies:

- a. The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- b. The data subject has given their consent.
- c. The transfer is necessary for one of the reasons set out in the Data Protection Requirements, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- d. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- e. The transfer is authorised by the relevant data protection authority and we have provided adequate safeguards to protect the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold might also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff might be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details or the provision of support services.

SIGNED BY

on *(enter date)*

FULL NAME (IN CAPITAL LETTERS):

Appendix 1: Schedule of Data Processing Activities

Type of Data	Data Subject	Type of Processing	Purpose of Processing	Recipient to whom data could be transferred	Retention Period
Name, Address, Contact Information, Salary, National Insurance Number.	Employees	Storage	Record keeping in line with business needs	HMRC	Entire employment period plus 2 years
Name, address, contact information (including secondary), notes, referral / application forms, actions and activity, mentoring / team updates, Risks Assessment	Beneficiaries	Storage, information sharing where relevant and only to agreed designated persons, action planning	Record keeping in line with business needs Tracking progress, escalating issues / concerns, maintaining relationships and contact, communicating opportunities	Referring partners	Entire service user period plus up to 5 years
Name, Address, Contact Information, application forms/ Cvs, photos, references, DBS Checks	Volunteers	Storage	Record keeping in line with business needs communications, matching to volunteering opportunities	ILI for events and opportunities	Entire volunteering period plus 2 further years
Name, Address, Contact Information	Trustee Board	Storage	Record keeping in line with business needs	ILI for events and opportunities	Entire period of engagement plus 2 years
Name, Address, Contact Information	Steering Committee	Storage	Record keeping in line with business needs	ILI for events and opportunities	Entire period of engagement plus 2 years

Appendix 2: Relevant Contacts

Title	Name	Contact Details
CEO Inspiring Leadership Trust	Leigh Bowman-Perks	Inspiring Leadership Trust Data Protection Officer 53 London House, 172 Aldersgate Street, London EC1A 4HU leigh@inspiringleadershiptrust.com