Data Protection Policy 2022

Name of your organisation: The Jarrett Foundation

Name of designated Officer: Dr. Pearl Jarrett

Address: 40 Parkside Avenue, Bromley, Kent, BR1 2EJ

Telephone No: 0208 249 3915

Email: info@jarrettfoundation.org

Web Address: www.jarrettfoundation.org

All Jarrett Foundation staff and volunteers must sign or digitally acknowledge that they have received a copy of this policy. A register is kept by Dr. Pearl Jarrett of who has received a copy of this policy.

Table of Contents

1. Policy Statement:

The Jarrett Foundation seeks to comply with relevant legislation protecting privacy rights in every jurisdiction where the Organisation operates. The Jarrett Foundation's territorial scope is under the UK Data Protection legislation, and therefore this policy, applies to all processing of personal data by and for the Jarrett Foundation, regardless of where the processing takes place.

2. Data protection principles:

The Charity is committed to processing data in accordance with its responsibilities under the EU GDPR 2016/679 and the UK legislation Data Protection Act 2018.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed 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."

3. Data Protection Terminology:

Data Protection Regulation

Data Protection Regulation, can mean EU 2016/680 General Data Protection Regulations (GDPR) in Europe, or it can be the Data Protection Regulation 2018 UK.

Personal data

Personal data includes any information about a living person who can be identified. Personal data is made up of several pieces of information that, when put together, can be used to identify a specific person.

Sensitive personal data

Special kinds of personal data, known as sensitive personal data, are subject to additional safeguards. In general, organisations must have more compelling reasons to process sensitive personal data than they do with "ordinary" personal data.

Anonymous data

Some data sets can be changed in such a way that no persons can be recognised (directly or indirectly) from them by any means or by any person. It is a technically hard process to ensure that individuals cannot be identified.

Pseudonymous data

Without a "key" that permits the data to be re-identified, some collections of data can be changed in such a way that no individuals can be recognised from them (directly or indirectly). Coded data sets used in clinical studies are a good example of pseudonymous data.

Data processing

The term "processing" includes a wide range of operations. It basically refers to anything that is done to or with personal information (including simply collecting, storing or deleting this data). This term is important because it indicates that EU data protection law will almost certainly apply whenever an organisation handles or affects personal data.

Controller

As compliance requirements under EU data protection law are principally imposed on controllers, the term "controller" was given special importance in the directive.

4. General provisions:

a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

5. Lawful, fair and transparent processing:

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

6. Lawful purposes:

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Charity shall note the appropriate lawful basis in the Register of Systems
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

7. Data minimisation:

The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

8. Accuracy:

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date

9. Archiving / Removal:

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

10. Security:

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

11. Breach:

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

12. What do you do if you believe there has been a data breach?

It is not the responsibility of the staff or Trustees working at The Jarrett Foundation to judge whether or not a data breach has taken place, but there are to act on any report with their line manager with the appropriate authorities so that they can make relevant enquiries and take the necessary action to protect the individuals concerned.

13. Who to inform, if you believe there has been a Data Breach:

Making a Report

In the first instance you should inform your line Manager, or contact Dr. Errord Jarrett.

In the email Header/Subject 'DATA BREACH REPORT', incident and date.

Name: (internal) Dr. Errord Jarrett
Email (internal) info@jarrettfoundation.org

CONFIDENTIALITY

Every effort should be made to ensure that confidentiality is maintained for the parties concerned. Information should be shared on a need-to-know basis only, and data kept in a secure place with limited access to designated people.

14. Disclosure and Barring Service (DBS).

The Jarrett Foundation uses the DBS Check Online Service (https://dbscheckonline.org.uk/) to help assess the suitability of staff whose roles brings them into contact with personal or sensitive data.

A Disclosure will only be requested after an assessment has indicated that it is both proportionate and relevant to the position concerned. An employee who refuses to undergo a DBS check will not be permitted to work on any project which involves direct access to personal or sensitive data.

Where a Disclosure forms part of the application process, the Jarrett Foundation encourages all applicants to provide details of their criminal record at an early stage in the application process. This should be sent under separate cover to your manager. Failure to reveal information that is directly relevant to the position sought, could lead to withdrawal of an offer of employment.

At interview, or in a separate discussion, the Organisation will ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. Having a criminal record will not necessarily bar an individual from working with the Organisation; the nature of the disclosed conviction and its relevance to the position will be considered. However, disclosure of previous offences involving identity theft, will result in withdrawal of an offer of employment in this area.

The Directors will undertake to discuss any matter revealed in a Disclosure with the person seeking a position with The Jarrett Foundation, before withdrawing a conditional offer of employment.

Signature: _____ **Date:** _____

Full Name and Title: _____

Position Applied or Volunteered For: _____

Support and Training:

We, The Jarrett Foundation, are committed to the provision of Data protection Training, in line with regulation for all our team members.

This policy was adopted on 30th October 2022 This policy will be reviewed on 30th October 2023

Signed:
Dr Pearl Jarrett, CEO, The Jarrett Foundation

USEFUL CONTACTS OR LINKS:

Information Commissioner's Office (ICO)
Website: https://ico.org.uk/

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

General Data Protection Regulations
Website: https://gdpr.eu/

GDPR.eu is a resource for organizations and individuals researching the General Data Protection Regulation. Here you'll find a library of straightforward and up-to-date information to help organisations achieve GDPR compliance.

Data Protection Act 2018
Web Link: https://www.gov.uk/data-protection

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

National Council for Voluntary Organisations
Web Link: https://www.ncvo.org.uk/help-and-guidance/digital-technology/data-protection-and-cybersecurity/#/

Charity Digital
Web Link: https://charitydigital.org.uk/cyber-security

Charity Digital produce advice that's designed with the needs of community groups and organisations in mind. The hub has the essential information you need to be secure; and we have webinars, training and skills sessions to take you beyond the basics.