Leavers Coulson Trust

Data Protection Policy

As individuals, we want to know that personal information about ourselves is handled properly and following Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulations (GDPR), we and others have specific rights in this regard. In the course of our activities the trust will collect, store and process personal data, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful organisation operations.

The types of personal data that we may be required to handle includes information about potential beneficiaries of grant support and applicants seeking grant support. Also details about supporters and donors, including volunteers and trustees. The personal data, which may be held on paper, computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and GDPR and other regulations. The Act imposes restrictions on how we may process personal data, and a breach of the Act could give rise to criminal sanctions as well as bad publicity.

Status of the policy

This policy has been approved by the trustees. It sets out our rules on data protection and the seven key principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation, storage and disposal of personal data.

Our office is responsible for ensuring compliance with the Act and with this policy. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the chair of trustees.

This policy is not part of the contract of employment and we may amend it at any time. However, it is a condition of employment that employees and others (volunteers and trustees) who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.

Any employee, volunteer or trustee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the chair of trustees.

Definition of the Data Protection Terms

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

Data users include employees and volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. Special Category data includes information about a person's race or ethnic origin, politics, religion, trade union membership, genetics or biometrics, or health or sex life, or sexual orientation. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the seven key principles of GDPR. These provide that personal data shall be:-

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Lawfulness, fairness and transparent

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness, transparency’)

Purpose limitation

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes

Data minimisation

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

Accuracy

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)”

Storage limitation

- 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 purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)

Integrity and confidentiality (security)

- 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'

Accountability

- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]

Fair and lawful Processing

The Act is intended not 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. The data subject must be told who the data controller is (in this case us), who the data controller's representative is (in this case the chairman of trustees), the purpose for which the data is to be processed by us and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, Relevant and Non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

The GDPR provides the following rights for individuals:-

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:-

- **Confidentiality** means that only people who are authorised to use the data can access it;
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

- Security procedures include:-
    - **Entry controls.** Any stranger seen in entry-controlled areas should be reported;
    - **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential);
    - **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required. Emails and related e-documents should be deleted.
    - **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock their computer when it is left unattended.

Dealing with subject access requests

A formal request from a data subject for information we hold about them must be made in writing to the office. Employees or volunteers who receive a written request should forward it to the chair of trustees immediately.

When receiving telephone or electronic enquiries, employees or volunteers should be careful about disclosing any personal information held on our systems. In particular they should:-

- Check the caller's identity to make sure that information is only given to a person who is entitled to it;
- Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked;
- Refer to the chair of trustees for assistance in difficult situations. Employees or volunteers should not feel pushed into disclosing personal information.

Our contact details are:-

The Administrator,
Leavers Coulson Trust,
1 Hall Close,
Henham
Bishop's Stortford
CM22 6AU
or
admin@leaverscoulsontrust.org.uk.