Poet in the City
Data Protection Policy

Introduction

This policy sets out the principles which the Charity intends to apply to the processing of personal data.

This policy applies to all of the Charity's staff. In this policy **staff** includes but is not limited to all employees, consultants, contractors, agency workers, homeworkers, interns, casual workers, volunteers and anyone else working on behalf of the Charity – i.e. anyone who is likely to come into contact with personal data which is being processed by the Charity.

All staff have a personal responsibility to ensure compliance with this policy (and related policies) and to handle all personal data consistently with the principles relating to the processing of personal data set out below. Senior individuals are expected to monitor and enforce compliance with this policy.

Any breach of this policy will be treated very seriously and may result in disciplinary action. If any member of staff becomes aware that the policy is being breached in any way, this should be reported to the CEO.

This policy is non-contractual and may be amended at any time. Any changes will be notified by email.

Technical terms

A number of terms applied in this policy are defined in the applicable legislation. Understanding the meaning of such terms may assist staff to comply with this policy, and their definitions are therefore set out at the end of the policy.

Overall responsibility for data protection within the Charity

The person with overall responsibility for data protection within the Charity and for upholding and enforcing the terms of this policy is the CEO. Staff should contact the CEO in relation to any data protection issues. In particular, any member of staff should contact the CEO immediately if he or she becomes aware:

- that anyone within the Charity is not complying or may not be complying with any part of this policy;
- that the Charity is engaging in a new processing activity or there has been a change to existing processing activities;
- of an actual or suspected personal data breach (please see "Reporting a Personal Data Breach" below for further information); or
- that a subject access request or other request to enforce rights available to data subjects under data protection legislation has been received by the Charity.

For the avoidance of doubt, the individual with overall responsibility for data protection within the Charity and for upholding and enforcing the terms of this policy is not a formal Data Protection Officer within the meaning of that phrase in applicable legislation.

Accountability

The Charity is responsible for ensuring compliance with the principles relating to the processing of personal data (which are set out below) and must also be able to demonstrate that it is compliant. It aims to do so by:

- drafting, maintaining and implementing various policies and procedures relating to personal data processing;
- arranging training for its members of staff in relation to data protection, as required, so that they understand their obligations and can work with the Charity to ensure that personal data is processed fairly and lawfully;
- maintaining records of its processing activities;
- implementing measures that meet the principles of data protection by design and default; and
- conducting due diligence on services providers who process personal data on the Charity's behalf, including taking reasonable steps to ensure those providers are capable of complying with the data protection principles, any data subject requests that the Charity may receive and any obligations under data protection legislation which the Charity may delegate to such service providers.

The data protection principles

In order to understand the obligations owed by both the Charity and its staff in relation to the processing of personal data, staff need to be aware of the six principles that underpin the lawful processing of personal data. These are set out below.

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness and transparency**);
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);
d) accurate and, where necessary, kept up to date (**accuracy**);
e) kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which the personal data is processed (**storage limitation**); and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or lawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures (**integrity and confidentiality**).

The steps adopted by the Charity to achieve compliance with each of these principles are set out below. All staff are required to adhere to the steps set out below.

Lawful, fair and transparent processing

For personal data to be processed lawfully, there must be a lawful basis for processing it. The Charity processes data because it is necessary:

- for the performance of contracts; or
- for compliance with any legal obligation to which it is subject; or

- for the purposes of the legitimate interests pursued by the Charity or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of the data subject.

In addition, the Charity may in certain circumstances rely on consent to process certain categories of personal data. For consent to be valid, it must be specific, informed, unambiguous and freely-given and the data subject has the right to withdraw that consent at any time (and must be advised of the right to do so). Where the Charity intends to rely on consent to process any particular category of personal data, this must be authorised by the CEO.

The Charity aims to be as transparent as possible in its processing of personal data and to ensure that data subjects are aware: that their personal data is being processed; which categories of personal data is being processed (including special category data where applicable) and on what lawful basis; which third parties receive it; how long it is retained and that they have certain rights under the applicable legislation. All this information is contained in the Charity's **Staff Privacy Notice**. These are available on request from the CEO.

Purpose limitation

The Charity aims only to process personal data for the legitimate purposes for which such data was collected, such purposes being specified in the applicable privacy notice. In particular, the Charity aims to limit the purposes for which it collects any special category data – for example, personal data in relation to sickness absence are collected in order to monitor attendance, process sick pay, to establish entitlement to any applicable benefits, and so that the Charity can comply with any obligations under the Equality Act 2010.

Should it no longer be necessary to process personal data for the purpose (or purposes) for which it was originally collected, it may be necessary to delete it in accordance with the Charity's **Data Retention Policy** which is available from the CEO. Alternatively, if the purpose for which the personal data is being processed has changed but processing is still legitimate, data subjects should be informed as soon as possible via an updated privacy notice. If an employee becomes aware that personal data is being processed for a reason other than that for which it was originally collected, s/he should notify the CEO.

Data minimisation

The Charity aims to limit its processing of personal data to circumstances where such processing is adequate, relevant and necessary for the purposes for which such data is being processed.

In particular, the Charity aims to limit its processing of special category data. Special category data in relation to staff will only be processed by the CEO and will be accessed only by individuals with the CEO's consent as appropriate.

Staff should only process personal data as is necessary in order to carry out their duties for the Charity and should avoid processing or disseminating personal data unnecessarily. For example, individual staff members should consider whether it is necessary:

- to retain multiple drafts (rather than the final version) of a document;
- for multiple staff (rather than a single staff member) to retain a copy of a particular document (or if only one person needs to keep it);
- to retain hard copies of a document if there is a soft copy;

- to copy multiple individuals on emails which contain personal data (in particular special category data); and
- to use "reply all" on emails containing such personal data.

Staff should not process any personal data on the Charity's systems that are unrelated to work. For example, staff should not send personal emails containing personal data from their work email account; or store personal data relating to their contacts on their work email folders or diary.

Accuracy

The Charity takes steps to ensure that the personal data which it processes are kept accurate and up-to-date. Staff are asked to notify the CEO if any of their contact or other personal details need to be updated.

Any member of staff who is processing personal data on behalf of the Charity is responsible for ensuring that such personal data is accurate at the point of collection, and that it is reviewed on a regular and systematic basis to ensure that it remains up-to-date.

If a member of staff becomes aware that any personal data processed by the Charity is inaccurate – whether his/her own, that of a colleague or that of a client or other third party, that member of staff must either ensure that it is corrected; or should contact the appropriate person or should contact the CEO if it may be appropriate for it to be deleted.

Storage limitation

A copy of the Charity's **Records Retention Policy** is available from the CEO. Staff are required to familiarise themselves with any relevant retention periods and to ensure that they adhere to them in respect of any personal data for which they are responsible. After the relevant retention period has expired, personal data should be permanently deleted in accordance with the terms of the Records Retention Policy.

Integrity and confidentiality

The Charity has put appropriate security in place to protect against data breaches. Those security measures include: password protected documents and systems, locked filing cabinets, available filing disposal methods. Where personal data, and in particular special category data is transferred to a third party, the Charity has satisfied itself that similar security measures are in place.

The Charity expects each staff member to use his or her best efforts to ensure that personal data is processed lawfully and securely. There are some simple steps which staff can take to help the Charity achieve this:

- operate a "clear desk" policy so that hard copy personal data is not left lying around;

- documents containing personal data, and in particular those containing special category data, should be stored securely. If they are in hard copy form they should be kept in a locked filing cabinet. Soft copy documents should also be stored securely by, for example, password protecting them or storing them in a folder with limited access;

- computers and hand held devices used for work purposes should be password protected with a sufficiently strong password. Passwords should never be shared. When a computer is

left unattended in the office, it should always be locked. A work computer or hand held device should never be left unattended outside the office;

- personal data should be saved only to designated drives and servers and should be uploaded only to an approved storage system. Staff must not save personal data locally or send it to their personal email addresses;

- personal data, and in particular special category data, should not be taken outside the office where this can be avoided. If this is necessary, such data should be treated with care and, if possible, password protected or encrypted soft copies should be taken outside the office rather than hard copies;

- if disposing of hard copy documents containing personal data, these should be shredded or disposed of via a confidential waste company;

- particular care should be taken when writing emails and documents which may contain personal data. Staff should consider whether it is necessary to include personal data (in particular if it is special category data). If so, staff should ensure that the content is appropriate and that the contents of such communication is suitable to be shared with the data subject; and

- particular care should also be taken, when writing an email which contains personal data, to ensure that it is only sent to appropriate recipients. Further care should be taken where recipients' names have been auto-filled.

Special Category Data

The Charity collects and processes certain categories of special category data for its staff, partners and audiences. Further details of the types of special category data the Charity processes and its lawful bases for doing so, are set out in the applicable privacy notice which is available from the CEO. The steps taken by the Charity to ensure that such special category data is processed in compliance with the data protection principles are set out above.

The retention periods for the categories of special category data processed by the Charity are set out in the Charity's Records Retention Policy which is available from the CEO.

International Transfers

The Charity does not transfer personal data outside the EEA.

Any member of staff who is required to transfer data out of the EEA should be clear that there is authorisation to do so. If in any doubt, the matter should be referred to the CEO.

Sharing personal data

The Charity is generally not permitted to share personal data with a third party unless certain safeguards and contractual arrangements are in place so that it can be satisfied that third parties are processing personal data in compliance with data protection legislation.

Members of staff should not share personal data with third parties where there is no business need to do so.

Any member of staff who is required to share personal data with a third party should be clear that there is authorisation to do so. If in any doubt, the matter should be referred to the CEO.

Reporting a personal data breach

Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed by, or on behalf of, the Charity. Examples of a personal data breach include but are not limited to:

- personal data being lost, or left in an unsecure location (for example, on an unattended desk, or on public transport);
- deletion of data either accidentally or by an unauthorised person;
- unauthorised access to the Charity's office;
- a hacking attack into the Charity's ICT systems;
- a letter containing personal data being sent to the wrong address;
- an email containing personal data being sent to the wrong recipients, such as where an email is sent "cc all" to people who should not have been copied;
- loss or theft of a mobile device or other ICT equipment containing personal data;
- the introduction of malware (including ransomware) or other viruses to ICT systems; and
- unauthorised or accidental alteration of personal data.

If a member of staff discovers or receives a report of an actual or suspected personal data breach, the CEO must be informed immediately. If the incident occurs or is discovered outside normal working hours, staff should email the CEO at isobel@poetinthecity.co.uk. Details of the breach should be notified to the CEO by completing the form (to the extent possible) attached in the Appendix to this policy.

If the Charity discovers that there has been a personal data breach that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Charity will record all personal data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Staff must be open and transparent with the CEO about any actual or potential data breach. There will be no repercussions for any member of staff who reports a suspected personal data breach in good faith, even if on investigation such suspected breach is found not to be an actual breach. A member of staff who fails to report an actual or suspected personal data breach (of which such staff member is aware) or fails to do so in a timely manner, however, may be subject to disciplinary action. Details of any actual or suspected personal data breach, the notification of such breach and any investigation should be kept confidential. Breach of confidentiality may give rise to disciplinary action. However nothing in this paragraph shall prevent a member of staff from making a protected disclosure under Part 4A of the Employment Rights Act 1996.

Data subjects rights

Data subjects have various rights under the applicable data protection legislation and these are set out in the Charity's privacy notices. Further information is also available from the ICO website

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

Further information

The Charity promotes transparency in its processing of personal data. If any member of staff has any questions about this policy, please contact Isobel Colchester (CEO) at isobel@poetinthecity.co.uk.

Defined terms

Controller: the entity which alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this policy, the Controller is the Charity.

Personal data: 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 breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by 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.

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

Special Category Data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third Party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.