Data Protection Policy Statement

The Polehampton Charity (the Charity) is committed to complying with privacy and data protection laws including:

(a) the General Data Protection Regulation (the GDPR) and any related legislation which applies in the UK including the Data Protection Act 2018 (the DPA);
(b) the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including E-Privacy Regulation 2017/0003; and
(c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and the guidance and codes of practice issued by the Information Commissioner's Office or any other supervisory authority.

This policy sets out what the Charity does to protect individuals' personal data.

Anyone who handles personal data in any way on behalf of the Charity must ensure that they comply with this policy. The policy outlines the definition of "personal data". Any breach of this policy will be taken seriously.

Data Protection Policy

About this policy

The types of personal data that the Charity may handle include details of grant applicants/recipients, Trustees, partners, stakeholders and associated individuals.

The Clerk to Trustees is the Data Protection Officer (DPO) for the Charity and is responsible for ensuring compliance with the DPA and with this policy.

Any questions or concerns about this policy should be referred in the first instance to the DPO.

Processing data fairly and lawfully

The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

To comply with this principle, every time the Charity receives personal data about a person directly from that individual, which the Charity intends to keep, the Charity needs to provide that person with "the fair processing information". In other words, the Charity needs to tell them:

(a) The type of information that will be collected (categories of personal data concerned);
(b) Who will be holding their information, namely the Charity including contact details and the contact details of its DPO;
(c) Why the Charity is collecting this information and what the Charity intends to do with it, for instance to process grant applications, make payments or send them mailing updates about the Charity's activities;
(d) The legal basis for collecting the information (for example, is the Charity relying on their consent, or on its legitimate interests or on another legal basis);
(e) If the Charity is relying on legitimate interests as a basis for processing what those legitimate interests are;
(f) Whether the provision of personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
(g) The period for which personal data or data will be stored or, where that is not possible, the criteria that will be used to decide that period;
(h) Details of people or organisations with whom the Charity will be sharing personal data;
(i) If relevant, the fact that the Charity will be transferring personal data outside the EEA (European Economic Area) and details of relevant safeguards; and
(j) The existence of any automated decision-making including profiling in relation to that personal data.

Where the Charity to obtain personal data about a person from a source other than the person his or herself, the Charity must provide that individual with the following information in addition to that listed above:

(a) The categories of personal data held; and

(b) The source of the personal data and whether this is a public source.

The Charity must also inform individuals of their rights outlined in this policy.

Processing data for the original purpose

The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when the Charity first obtained their information.

This means that the Charity should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if the Charity collects personal data such as a contact number or email address, in order to update a person about the Charity's activities it should not then be used for any new purpose, for example, to share it with other organisations for marketing purposes, without first getting the individual's consent.

Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data that the Charity keeps should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and the Charity must take every reasonable step to ensure that personal data which is inaccurate is corrected.

Not retaining data longer than necessary

The fifth data protection principle requires that the Charity should not keep personal data for longer than is needed to for the purpose it was collected for. This means that the personal data that the Charity holds should be destroyed or erased from its systems when it is no longer needed. If you think that the Charity is holding out-of-date or inaccurate personal data, speak to the DPO.

For guidance on how long particular types of personal data that the Charity collects should be kept before being destroyed or erased, see the Charity's Data Retention Policy.

Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of the Charity needs to be aware of these rights.

They include (but are not limited to) the right:

(a) to request a copy of any personal data that the Charity holds about them (as data controller) as well as a description of the type of information that the Charity is processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);
(b) to be told, where any information is not collected from the person directly, and any available information as to the source of the information;
(c) to be told of the existence of automated decision-making;

(d) to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
(e) to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;
(f) to restrict processing where the individual has objected to the processing;
(g) to have inaccurate data amended or destroyed; and
(h) to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

Data security

The sixth data protection principle requires that the Charity keeps secure any personal data that it holds, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

With electronic records containing personal data, the following security procedures and processes will be followed:

- all organisation computers are to be anti-virus and firewall-protected with regular scans performed and remedial action taken;
- software updates are regularly installed;
- unique and strong passwords are to be used by all and never shared;
- all screens are to be locked when unattended; and
- all hardware is to be locked away when not in use.

With paper records containing personal data, the following security procedures and processes will be followed:

- all documents with sensitive data will be printed securely;
- all documents are locked away when not attended or in use;
- all documents being shared with partner organisations will be sent via secure delivery or in person; and
- all sensitive data will be shredded immediately after it is no longer required.

Using a personal device – all devices are to have their access secured with unique and strong passwords or PINs. When transporting devices, they are not to be displayed and hidden away where possible, for instance in the boot of a car. Devices are not to be stored in cars overnight.

Transferring data outside the EEA

The Charity will only transfer personal data outside the EEA if the contract between the organisations includes adequate security measures for personal data.

The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but this list may be updated. Personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation.

The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the DPO before transferring personal data to organisations in the US.

Processing sensitive personal data

Due to the nature of the Charity work as an alternative education provider for young, often vulnerable adults, it collects and processed information about individuals that is defined by the GDPR as special categories of personal data, and special rules will apply to the processing of this data. In this policy "special categories of personal data" is referred to as "sensitive personal data".

The legal basis that the Charity relies on for processing much of this sensitive personal data is that it has a legal obligation as an alternative education provider. The Charity's privacy statements will capture the legal basis for all data processing in sufficient detail.

Notification of breach

The Charity will implement a systematic process for enabling breach detection and assessing the impact of breaches. Breaches will be responded to appropriately and within a timely manner. A comprehensive action plan is to be maintained and implemented in the event of a significant data breach.

The Charity will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. The Charity will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals. Any third party with whom the Charity shares the data with will also be notified.

Monitoring and review of this policy

This policy and statement are to be reviewed by the DPO to ensure they are achieving their objectives using the annual monitoring and review cycle.