GDPR POLICY AND PROCEEDURES

PANTRY will ensure that all personal data that it holds will be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary;
- 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.

GDPR OPERATIONAL POLICIES AND PROCEEDURES-THE CONTEXT

PANTRY is a small charity holding minimal amounts of non-sensitive data on a small number of people.

The Trustees understand and accept their responsibility under the UK General Data Protection Regulation (UK-GDPR) to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of the data subjects.

By the following operational policies and procedures the Trustees undertake to uphold the principles and requirements of the UK-GDPR in a manner which is proportionate to the nature of the personal data being held by the Charity. The policies are based on the Trustees' assessment, in good faith, of the potential impacts on both the Charity and its data subjects of the personal data held by the Charity being stolen, abused, corrupted or lost.

PERSONNEL WITH RESPONSIBILITY FOR GDPR

Data Protection Officer:

Although in the opinion of the Trustees the scope and nature of the personal data held by PANTRY is not sufficient to warrant the appointment of a Data Protection Officer, we have decided that a Data Protection Officer will be appointed.

Data Controller:

The Board of Trustees is the Data Controller for the Charity.

Data Processor:

The Board of Trustees will delegate the role of data processor to the management committee who will appoint an appropriate person, to be the Data Processor for the Charity.

The Charity will not knowingly outsource its data processing to any third party (eg: Google G-Suite, Microsoft OneDrive) except as provided for in the section "Third Party Access to Data".

Access to Data:

Except where necessary to pursue the legitimate purposes of the Charity, only the Data Processors shall have access to the personal data held by the Charity.

Training:

The Board of Trustees and Data Processor will periodically undergo appropriate training commensurate with the scale and nature of the personal data that the Charity holds and processes under the UK-GDPR.

COLLECTING AND PROCESSING PERSONAL DATA

PANTRY collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of its charitable objects.

All personal data will be collected, held and processed in accordance with the relevant Data Privacy Notice provided to data subjects as part of the process of collecting the data.

A Data Privacy Notice will be provided, or otherwise made accessible, to all persons on whom the Charity collects, holds and processes data covered by the UK-GDPR. The Data Privacy Notice provided to data subjects will detail the nature of the data being collected, the purpose(s) for which the data are being collected and the subjects rights in relation to the Charity's use of the data and other relevant information in compliance with the prevailing UK-GDPR requirements.

INFORMATION TECHNOLOGY

Data Protection by Design/Default:

In as much as:

a) None of the Charity's volunteer Trustees or Management Team are data protection professionals;

b) It would be a disproportionate use of charitable funds to employ a data protection professional, given the scale and nature of the personal data held by PANTRY;

The Trustees/Management Committee will seek appropriate professional advice commensurate with its data protection requirement whenever:

c) They are planning to make significant changes to the ways in which they process personal data;

d) There is any national publicity about new risks (e.g.: cyber-attacks);

e) Any material changes to the UK-GDPR are proposed or have been made which might adversely compromise the Charity's legitimate processing of personal data covered by the UK-GDPR.

Personal data will never be transmitted electronically (e.g.: by e-mail) unless securely encrypted.

DATA PROCESSING EQUIPMENT

The scale and nature of the personal data held by the Charity is not sufficient to justify the Charity purchasing dedicated computers for the processing of personal data at its site of operations.

Instead the Charity will purchase and own at least 3 and not more than 5 storage devices/laptops to store the personal data that it holds and processes.

The storage devices/laptops will also act as backup devices with data being stored in a secure cloud based system.

Whilst the data will be processed on the computers/laptops to which the Data Processors have access, no personal data covered by the UK-GDPR will be stored on those computers/laptops. All interim working data transferred to such computers/laptops for

processing will be deleted once processing has been completed and saved to the secure cloud based storage.

When not in use the storage devices/laptops will be kept in a secure location and reasonably protected against accidental damage, loss, avoidable theft or other misuse by persons other than the Data Processors.

The Data Controller & Data Processors will keep a register of

The location of all devices used for the storage and processing of personal data;

The Charity's storage devices/laptops shall not be used for the storage of any data which are unrelated to the Charity's processing of personal data or for the storage of personal data.

DATA PROCESSING LOCATION

Data Processors shall only process the Charity's personal data in a secure location, and not in any public place, e.g.: locations whether the data could be overlooked by others or the data storage devices/laptops would be susceptible to loss or theft.

Computers/laptops in use for data processing must be adequately protected with strong passwords and not be left unattended at any time.

DATA BACKUPS

To protect against loss of data by accidental corruption of the data or malfunction of a data storage device/laptop (including by physical damage), all the Charity's personal data shall be backed up to a cloud based storage facility and whenever any significant changes (additions, amendments, deletions) are made to the data.

DATA SUBJECTS

THE RIGHTS OF DATA SUBJECTS

In compliance with the UK-GDPR the Charity will give data subjects the following rights.

These rights will be made clear in the relevant Data Privacy Notice provided to data subjects:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right of erasure; also referred to as "The right to be forgotten"
- The right to restrict processing;
- The right to data portability;
- The right to object;

- The right not to be subjected to automated decision making, including profiling.

RIGHTS OF ACCESS, RECTIFICATION AND ERASURE

Data subjects will be clearly informed of their right to access their personal data and to request that any errors or omissions be corrected promptly.

Such access shall be given and the correction of errors or omissions shall be made free of charge provided that such requests are reasonable and not trivial or vexatious.

There is no prescribed format for making such requests provided that:

a) The request is made in writing, signed & dated by the data subject (or their legal representative);

b) The data claimed to be in error or missing are clearly and unambiguously identified;

c) The corrected or added data are clear and declared by the subject to be complete and accurate.

It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate volunteers or staff to deal with the request do not work on every normal weekday.

Where a data subject requests that their data be rectified or erased the Data Controller and Data Processor will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data including those copies which are in the hands of a Third Party for authorised data processing.

RIGHT OF PORTABILITY

The Charity will only provide copies of personal data to the subject (or the subject's legal representative) on written request.

The Charity reserves the right either:

a) To decline requests for portable copies of the subject's personal data when such requests are unreasonable (i.e.: excessively frequent) or vexatious;

OR

b) To make a reasonable charge for providing the copy.

DATA RETENTION POLICY

Personal data shall not be retained for longer than:

a) In the case of data held by subject consent:

The period for which the subject consented to the Charity holding their data;

b) In the case of data held by legitimate interest of the charity:

The period for which that legitimate interest applies. For example: in the case of data subjects who held a role, such as a volunteer, with the Charity the retention period is that for which the Charity reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it;

c) In the case of data held by legal obligation:

The period for which the Charity is legally obliged to retain those data.

The Charity shall regularly – **not less than every 6 months** – review the personal data which it holds and remove any data where retention is no longer justified. Such removal shall be made as soon as is reasonably practical, and in any case no longer than 20 working days (of the relevant Data Processor) after retention of the data was identified as no longer justified.

PRIVACY IMPACT ASSESSMENT

Trustees' Data:

The volume of personal data is very low – less than 10 individuals

The sensitivity of the data is moderate: the most sensitive data being date of birth, names, phone numbers, email addresses and current addresses;

The risk of data breach is small as the data are rarely used, with the majority of the data being held for a combination of legal obligation and legitimate interest.

Overall impact: LOW

Volunteers'/Members' Data:

The volume of personal data is low – less than 100 individuals

The sensitivity of the data is moderate: the most sensitive data being date of birth, names, phone numbers, email addresses and current addresses;

The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

Supporters' & Enquirers' Data:

The volume of personal data is low-moderate.

The sensitivity of the data is low: the most sensitive data being names, phone numbers, email addresses and current addresses;

The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

THIRD PARTY ACCESS TO DATA

Under no circumstance will the Charity share with, sell or otherwise make available to Third Parties any personal data except where it is necessary and unavoidable to do so in pursuit of its charitable objects as authorised by the Data Controller.

Whenever possible, data subjects will be informed in advance of the necessity to share their personal data with a Third Party in pursuit of the Charity's objects.

Before sharing personal data with a Third Party the Charity will take all reasonable steps to verify that the Third Party is, itself, compliant with the provisions of the UK-GDPR and confirmed in a written contract.

The contract will specify that:

- The Charity is the owner of the data;
- The Third Party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller;
- The Third Party will not use the data for its own purposes;
- The Third Party will adopt prevailing industry standard best practice to ensure that the data are held securely and protected from theft, corruption or loss;
- The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of the Charity's data (including any fines or other penalties imposed by the Information Commissioner's Office) unless such theft, breach, corruption or loss was a direct and unavoidable consequence of the Third Party complying with the data processing instructions of the Data Controller
- The Third Party will not share the data, or the results of any analysis or other processing of the data with any other party without the explicit written permission of the Data Controller;
- The Third Party will securely delete all data that it holds on behalf of the Charity once the purpose of processing the data has been accomplished.
- The Charity does not, and will not, transfer personal data out of the UK.

DATA BREACH

In the event of any data breach coming to the attention of the Data Controller the Trustees will immediately notify the Information Commission's Office.

In the event that full details of the nature and consequences of the data breach are not immediately accessible (e.g.: because Data Processors do not work on every normal weekday) the Trustees will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available.

All necessary steps to prevent further breaches of data will be investigated and initiated.

PRIVACY POLICY AND PRIVACY NOTICES

The Charity will have a Privacy Policy and appropriate Privacy Notices which it will make available to everyone on whom it holds and processes personal data..

In the case of data obtained directly from the data subject, the Privacy Notice will be provided at the time the data are obtained.

> In the case that the data are not obtained directly from the data subject, the Privacy Notice will be provided within a reasonable period of the Charity having obtained the data (within one month),
>
> OR
>
> If the data are used to communicate with the data subject, at the latest, when the first communication takes place;
>
> OR
>
> If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

REVIEW

This policy will be reviewed every two years

Date……..

Signature (Chair)……..

Signature (Secretary)……