Data retention policy

Overview

Key details

- Policy prepared by: Hugh Parry
- Approved by Trustees on: 25/05/2018
- Next review date: 25/05/2019

Introduction

This policy sets out how the Trust will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of the Trust Data Protection Policy.

Roles and responsibilities

The Trust is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for the Trust is the Treasurer. He/she and the Trustees are responsible for the secure and fair retention and use of data by the Trust. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

Regular Data Review

A regular review of all data will take place to establish if the Trust still has good reason to keep and use the data held at the time of the review.

As a general rule a data review will be held every 2 years and no more than 27 calendar months after the last review. The first review will take place by 25 May 2018.

Data to be reviewed

- The Trust stores data on digital documents (e.g. spreadsheets) stored on personal devices held by trustees and officers.
- Data stored on third party online services (e.g. Google Drive, Mail Chimp)
- Physical data stored at the homes of trustees and officers.

Who the review will be conducted by

The review will be conducted by the Data Protection Officer with other committee members to be decided on at the time of the review.

How data will be deleted

- Physical data will be destroyed safely and securely, including shredding.
- All reasonable and practical efforts will be made to remove data stored digitally.
    - Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.
    - Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Criteria

The following criteria will be used to make a decision about what data to keep and what to delete.

Question	Action	
	Yes	**No**
Is the data stored securely?	No action necessary; move to the next question in the flow chart	Update storage protocol held by the data protection officer in line with Data Protection policy and remove any data which is no longer in line with the GDPR guidelines
Does the original reason for having the data still apply?	Continue to use	Delete or remove data
Is the data being used for its original intention?	Continue to use	Either delete/remove or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data unless we have reason to keep the data under other criteria.
Is the data accurate?	Continue to use	Ask the subject to confirm/update details
Where appropriate, do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent or remove the data immediately
Can the data be anonymised	Anonymise data	Continue to use

Statutory Requirements

Date stored by the Trust may be retained based on statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declarations records

- Details of payments made and received (e.g. in bank statements and accounting records)
- Trustee meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax records

Other data retention procedures

Audience member data

- When an audience member leaves the Trust and all administrative tasks relating to their membership have been completed any potentially sensitive data held on them will be deleted – this might include bank details or medical data
- Unless consent has been given, data will be removed from all email/mailing lists
- All other data will be stored safely and securely and reviewed as part of the next two-year review

Mailing list data

- If an individual unsubscribes of a mailing list their data will be removed as soon as is practically possible.
- All other data will be stored safely and securely and reviewed as part of the next two-year review

Volunteer and freelancer data

- When a volunteer or freelancer stops working with the Trust and all administrative tasks relating to their work have been completed any potentially sensitive data held on them will be deleted – this might include bank details or medical data
- Unless consent has been given data will be removed from all email/mailing lists
- All other data will be stored safely and securely and reviewed as part of the next two-year review

Other data

All other data will be included in a regular two-year review.