CART HORSE PROTECTION ASSOCIATION

DATA PROTECTION POLICY

Created :	September 2024
Last Revised:	
Review Date :	September 2026

Data Protection Policy

Introduction
This policy is about data. It covers personal data and other organisational data including intellectual property. It covers the Cart Horse Protection Association's (CHPA) policy on keeping information safe.

Personal data is defined as information which can identify a living individual. This can include a name, address, location indicator, photographs etc. This information is stored by the organisation with the intention of being accessed again. It includes electronic or hard copy data. The protection of Private Information Act (POPIA) restricts the definition to information about a living individual. The information covered includes not just facts but interpretation and comment – for example whether we would consider employing a candidate or comments by a solicitor on details of a bequest etc.

CHPA needs to collect, process and use certain types of information, for example on current, past and prospective employees, members, suppliers, adopters, customers, donors, volunteers, beneficiaries and supporters, and others with whom it communicates. It may be required to collect and use certain types of information to comply with legal and regulatory requirements. Other information is held by the organisation in order to run the organisation effectively; this includes welfare, financial, fundraising, IT, intellectual property and governance data. Much of the data has a value, such as intellectual property or copyright and as an asset of the organisation it must be safeguarded.

In this policy the word "data" is used to include all these types of information. This data must be dealt with properly irrespective of how it is collected, recorded, used and disposed of.

All staff are responsible for the successful implementation of this policy and should ensure that they take the time to read and understand it. Compliance with the Communications E-mail and Internet and POPIA and Privacy Policy is essential for compliance with this policy.

1. Policy
The organisation regards the lawful and correct treatment of data as critical to successful operations, and to maintaining the public's confidence.

To maintain the organisation's reputation and integrity it fully endorses and adheres to the principles of data as set out in the POPIA.

The organisation will:
- Be clear about why it is collecting and keeping data and get fresh consent if the use of personal data is materially changed
- Collect and process data only to the extent that it is needed as part of the work of the organisation or to comply with legal requirements
- Carry out checks to ensure the accuracy of the data it keeps and correct errors
- Keep the data secure
- Check to ensure data is held for the right length of time. See Appendix 1.
- Destroy data securely when it should no longer keep it
- Ensure that people consent to their data being held and can get copies of information about themselves
- Ensure that data is not transferred without suitable safeguards and encryption
- Take appropriate technical and organisational security measures to safeguard data

- Use appropriate Intellectual Property and Copyright legislation to protect its original ideas and other work
- Make sure appropriate data processing agreements are in place if we do share data
- Make sure that the data subject is aware about how we use, share, process their data and give them opportunities to change this

2. Personal data held by the organisation

There are six lawful bases for the organisation to hold personal data and use it ("processing"):

- Consent
- Legitimate interest (the individual would reasonably expect this)
- Contractual reason (e.g. provision of a service)
- Public interest
- Vital reason (e.g. life and death situation)
- Legal reason

Staff need to understand which is appropriate to their area of work and also that the processing is necessary through one of the following reasons:

- In relation to a contract which the individual has entered into
- Because the individual has asked for something to be done so they can enter into a contract
- To fulfil a transaction
- To fulfil a legal obligation that applies to the organisation
- There is a legitimate interest in holding the data which outweighs the interest of the individual

Information collected or stored from children under-18 requires parental or guardian consent. It is also necessary to secure a birth date, as consent passes to the child when they reach 18.

3. Sensitive personal data

Sensitive personal data requires more exacting conditions. Unequivocal explicit consent is required and processing must be necessary to protect the individual or for legal or regulatory purposes imposed on the organisation in connection with employment. Such data is mainly information about:

- Ethnic background
- Religious belief
- Political opinion
- Health (a dietary requirement could be viewed as sensitive personal data)
- Criminal records

It must not be processed without the prior consent of the General Manager.

4. Staff responsibilities

Staff whose role includes the management of data should also:

- Be able to report on compliance to the General Manager when requested
- Establish and maintain procedures to check data accuracy, security and relevance
- Make arrangements to store and destroy data appropriately. See Appendix 1

All staff should ensure that data handled in the course of their work is:

- Accurate
- Secure – locked away or password protected
- Not left out when they are away from the desk for an extended period or overnight
- Not accessible on screen for unauthorised users

5. Data breach

Any breach or loss of data needs to be reported to the General Manager who will determine the consequent course of action.

6. Subject access requests

All requests must be passed to the General Manager. Some information may be withheld (e.g. for example if it concerns a prosecution case).

7. Third party access requests

Requests must be passed to the General Manager. Data will be passed to third parties where there is a legal or regulatory requirement. Other requests will be considered individually.

8. Information about employees

CHPA will keep information about its employees which includes:

- Name
- Address
- Phone number
- Date of birth
- Gender
- Education and qualifications
- Work experience
- Identity number and tax code
- Identity copy
- Disability
- Emergency contact details
- Employment history with the organisation
- Terms and conditions
- Accidents
- Training
- Disciplinary action

Staff will be asked periodically to check the accuracy of the information and may ask to review it at any time. Staff information will be securely shared with providers where appropriate based on contractual or legal basis to administer payroll, pensions and other staff benefits or training.

Cart Horse Protection Association
Data Protection Policy

Declaration

I acknowledge that I have read and understood the Cart Horse Protection Association's Data Protection Policy.

I agree to comply with the contents of the Policy and understand that failure to do so may result in disciplinary or legal action.

Signature: _____

Name: _____

Date: _____

Appendix 1: Proposed minimum data retention periods

Retention periods vary given the particular situation. For example:

- Intellectual property agreement and licences – 6 or 12 years after expiry
- All contracts with adopters, customers and suppliers -10 years after expiry
- Financial information – 7 years after expiry, as per the SARS requirement
- Pledged legators – for as long as is necessary to receive and administer the gift
- Welfare cases – 20 years after the last concern (due to the expected life of an equid) , unless it is a prosecution
- Legacy information – 7 years after the Will has been proven or as long as is necessary
- Donations – 20 years after the last transaction
- Agreements with architects and builders – 6 years after completion or as long as is necessary
- Job application and interview notes – 3 months after notifying unsuccessful candidates or as long as is necessary
- HR staff information after staff have left – 7 years or as long as is necessary
- Training records relating to safety at work – permanently

All information of a confidential or sensitive nature on any media of any sort should be securely destroyed when it is no longer required, when the legal or regulatory requirement to keep it has ceased.

In addition there is data (which includes personal data) which may be significant in terms of the governance, management, history or development of the organisation (e.g. minutes, accounts or financial, legal or disciplinary) or of important policy changes or initiatives (e.g. minutes of policy forming groups, policy papers and correspondence). These should be retained for as long as is necessary where the data:

- Would be useful for retrospective comparisons (e.g. annual reports and statistics)
- Was gathered from outside the organisation and is likely to be of use to future historians, and is not readily available elsewhere (e.g. statistics relating to petitions, international courses, campaign Information and analysis)
- Is likely to be useful as legal evidence in the future (e.g. papers relating to disputes (but only those which record the outcome and significant events leading to it))
- Is likely to be of use to future researchers, and which is not covered by the preceding categories (e.g. surveys of buildings or land)