Hungerford
youth and community
Charity no.11846921

Data protection Policy including Key Procedures

Version:	V0.1
Date approved:	15/06/2023
Approved by:	Board of Trustees
Date of last update:	
Period for review:	Every three years
Policy Scope:	Organisation wide
History of changes:	-

1. Aim of the Policy

HYCC needs to keep certain information on its employees, volunteers, trustees and service users (hall hirers and youth club members) to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers staff, trustees and volunteers.

2. Definition of Data Protection

In line with the Data Protection Act 1998 principles, HYCC will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability**: those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility**: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained, except in case of an emergency or safeguarding concern.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

3. Type of information processed

HYCC processes the following personal information:

- Information on applicants for posts, including references
- Employee information – contact details, bank account number, payroll information, supervision and appraisal notes.
- Volunteer – contact details
- Trustee – contact details
- Service users – contact details

Personal information is kept in the following forms:

- On Paper based forms
- Detailed in Computer based systems

Groups of people within the organisation who will process personal information are:

- Employed staff,
- Trustees
- Volunteers – only those who have had the relevant training.

4. Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a voluntary organisation rests with the governing body. In the case of HYCC, this is the Board of Trustees.

All employed staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings.

5. Policy implementation

To meet our responsibilities staff, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

6. Training

Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

On induction:

As part of their training, every member of staff is told that personal information must be kept securely in digital form. Paper copies need to be manually transferred to digital records and the paper copies destroyed securely.

General training/ awareness raising: annual reminders about the policy in a team meeting or supervision meeting.

7. Gathering & checking information

Before personal information is collected, we will consider:

- What details are necessary and for what purposes
- How long we are likely to need this information

We will inform people whose information is gathered about the following:

- why the information is being gathered;
- what the information will be used for;
- who will have access to their information (including third parties).

We will take the following measures to ensure that personal information kept is accurate:

- Send out annual reminders to ask people to check their details.
- All youth club members' contact information will be deleted in September each year and new registration forms collected.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

8. Retention period

HYCC will ensure that information is kept according to the following retention periods guidelines:

- Personnel files -6 years after employment/volunteering ceases, (slimmed down format after 2 years);
- Application forms and interview notes (unsuccessful candidates)- 1 year;
- Letters of reference - 6 years from the end of employment;
- Redundancy details -6 years from the date of redundancy;
- Parental leave - 5 years from birth/adoption or 18 if child receives a disability allowance;
- Accident books, accident records/reports - 3 years;
- Assessments under health & safety regulations- Permanently;
- Income tax, NI returns, income tax records and correspondence with HMRC - At least 5 years after the end of the financial year to which they relate;
- Statutory maternity pay records and calculations - At least 3 years after the end of the financial year to which they relate;
- Statutory sick pay records and calculations - At least 3 years after the end of the financial year to which they relate;
- Wages and salary records - 6 years;
- Employee joining/new starter form - 6 years after employment ceases;

- Project information on service users - Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. For European Funded projects this can be up to 13 years.

9. Data security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using lockable cupboards (restricted access to keys);
- Password protection on personal information files;
- Setting up computer systems to allow restricted access to certain areas;
- Personal data can be taken off site, in paper, memory stick, laptop and work phone. Paper copies need to be kept in a lockable cupboard and all digital devices are password protected;
- All work devices can be remotely locked and all accounts logged out;
- Back up of data on computers (onto a server/the cloud off site);
- Password protected attachments for sensitive personal information sent by email.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

The Board and trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

10. Procedure in case of breach

When a breach of data protection occurs, consideration will be given to reviewing practices. In addition, HYCC will consider whether the breach should be reported to the Information Commissioner and/or to any partners with which we hold Information Sharing or Partnership Agreements.

11. Subject access requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the HYCC director: office@hungerfordyc.org.uk

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- their relationship with the organisation (former/ current member of staff, trustee or other volunteer, service user)

We may also require proof of identity before access is granted. The following forms of ID will be required: e.g. passport, birth certificate.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

12. Review

This policy will be reviewed every three years to ensure it remains up to date and compliant with the law.