Data Protection Policy

Introduction

We hold personal data about our workforce, customers, donors, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our workforce understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires our workforce to ensure that the Data Compliance Officer (DCO) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Personal data	Information relating to identifiable individuals, such as members, customers, participants, donors, job applicants, current and former employees and volunteers, agency, contract and other staff, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings – any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all our workforce. Staff and volunteers must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff and volunteers before being adopted.

Who is responsible for this policy?

As our Data Compliance Officer (DCO), Paula Thomas has overall responsibility for the day-to-day implementation of this policy. Details of specific responsibility of the DCO and other key staff are set out later in this policy.

Our policy

We will process personal data in compliance with these data protection principles:

- Fair and lawful
- Specific and lawful purposes
- Adequate, relevant and not excessive
- Accurate and, where necessary, kept up-to-date
- Keep no longer than is necessary
- Rights of Data Subjects
- Appropriate technical and organisational security measures
- Not to be transferred to a country or territory outside the European Economic Area unless adequate protections are in place.

We will document the additional justification for the processing of sensitive data.

Fair and lawful processing

We will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening or we have another legal basis for processing.

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice which will be provided to all date subjects when data is collected and is available on our website.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Data retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the

personal data was obtained, but should be determined in a manner consistent with our data retention guidelines which can be found on our website.

Rights of Data Subjects
We will ensure that the rights of data subjects as set out in the data protection legislation are respected and adhered to:

- subject access
- to have inaccuracies corrected
- to have information erased
- to prevent direct marketing
- to prevent automated decision –making and profiling
- data portability

Data security
We will ensure that all personal data is held secure against loss or misuse.
Where other organisations process personal data as a service on our behalf, the DCO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

International data transfers
We will ensure that no data is be transferred outside the EEA for processing without the consent of the data subject and without first being discussed with the DCO.

Finding out more
To find out what information the Horniman holds about you, you will need to submit a subject access request to the Data Compliance Officer. You can do this in several ways:

- Complete and return the Subject Access Request form
- email the Data Compliance Officer enquiry@horniman.ac.uk
- in a letter, addressed to:

  Data Compliance Officer
  Horniman Museum and Gardens
  100 London Road
  London SE23 3PQ

Please provide as much detail as possible to help us answer your request.

You can also contact the Data Compliance Officer if you want to:

- ask us to correct any mistakes
- find out how we check the information we hold is accurate and up-to-date
- ask us to remove any information we hold about you
- ask us to transfer any information we have about you to another system
- find out what agreements we have with other organisations for sharing information
- find out in what circumstances we can pass on your personal information without telling you, for example to prevent and detect crime or to produce anonymised statistics
- find out what guidance is given to Horniman staff about handling personal information.

We will acknowledge your request within 5 working days of receipt and provide you with a response within 30 days. All information is provided free of charge.