

Data Protection and Confidentiality

Approved by the Trustees of Hertford Museum

Date:

Introduction

The purpose of this policy is to protect the rights of individuals about whom data (information) is obtained, stored, processed and disclosed by Hertford Museum.

What is this policy covering?

This policy establishes what may, and what may not, be done with personal information. Such personal information may be in electronic (e.g. stored on computer hard drive) or manual form (in a manual filing system).

The law

Hertford Museum is therefore required under law to comply with the General Data Protection Regulation GDPR. The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018. The legislation creates rights for those who have their data stored, and responsibilities for us who store, process or transmit such data. The person who has their data processed has the right to:

- View the data an organisation holds on them. A 'subject access request' can be obtained for a nominal fee. As of January 2014, the maximum fee is £10 per individual request.
- Request that incorrect information be corrected. If the company ignores the request, a court can order the data to be corrected or destroyed, and in some cases compensation can be awarded.
- Require that data is not used in any way that may potentially cause damage or distress
- Require that their data is not used for direct marketing

Consequences of breaching the Data Protection Act:

- Staff can be criminally liable if they knowingly or recklessly disclose personal data in breach of the Act.
- A serious breach of data protection is also a disciplinary offence and will be dealt with under Hertford Museum's disciplinary procedures. If a member of staff accesses another employee's personnel records without authority this constitutes a gross misconduct offence and could lead to summary dismissal.

Policy Statement

Hertford Museum is committed to fulfilling its legal obligations within the provisions of the Data Protection Act.

Access

Personal data may be normally held for less than 40 days, may be legitimately denied in subject access requests under the Act. It is a consequence of the time limit data controllers must meet in making their response. If the data has been deleted by the normal procedures of the business by the time the data controller responds to a request, that data cannot be supplied. For data such as closed-circuit television images, routinely overwritten, it may be impossible for a subject to exercise their data access rights.

An exception to this refers to collection donor's information which needs to be retained permanently.

The Eight Data Protection principles

There are eight principles of data (information) processing with which Hertford Museum as the data controller must ensure compliance.

Personal data shall be:

Principle 1: lawfulness, fairness and transparency

Principle 2: purpose limitation

Principle 3: data minimisation

Principle 4: accuracy

Principle 5: storage limitation

Principle 6: integrity and confidentiality

Accountability principle

Employment: Code of Practice

Hertford Museum will adhere to the Employment Codes of Practice on matters of:

- Recruitment and selection
- Employment records
- Monitoring at work

The Trustees of Hertford Museum have the responsibility for the implementation of these codes.

Compliance with data protection principles

Principle 1: Lawfulness, fairness and transparency

This means that when Hertford Museum is collecting personal information from individuals:

- that they are made aware of the uses of this information
- individual consent has been obtained for any secondary uses of their personal information
- individuals are made aware of disclosures of their personal information to third parties.

Information held by the organisation includes details on the following:

- customers and suppliers
- personnel
- applicants for recruitment and selection
- volunteers
- collection donors
- project/exhibition contributors
- mailing lists, including newsletter mailing list, Patrons of Hertford Museum, members of the Super 100 Club, Business Supporters, Trustees of Hertford Museum and voluntary donors who have provided their details for purposes of claiming gift aid

Hertford Museum processes sensitive data for the following purposes:

- Advice/legal proceedings
- Employment law obligations
- Vital interests of the data subject

- Legal rights
- Insurance and pensions

Principle 2: Purpose limitation

Personal information can only be obtained for one or more specified and lawful purposes and should not be processed in any manner incompatible with those purposes, that is:

- Staff administration
- Administration of membership records
- Fundraising
- Realising the objectives of a charitable organization, including volunteers management
- Administration of collections

Principle 3: Data minimisation

Hertford Museum will only hold personal information which is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. This means that the minimum of personal information should be held in order to fulfil its purpose. It is not acceptable to hold information on the basis that it might be useful in the future without a view of how it will be used. Hertford Museum has a responsibility to continually monitor compliance with this principle and to audit what information is kept.

Principle 4: Accuracy

This principle places a duty on Hertford Museum to take reasonable steps to ensure the accuracy of the information processed on the museum's information systems.

In collecting information Hertford Museum needs to take all reasonable steps to make sure the information is correct and the source of the information is reliable and to check this, if necessary.

Similarly, third parties who supply personal information to Hertford Museum should advise us of any corrections or amendments that need to be made.

The significance of the inaccuracy is important, obviously minor inaccuracies which have no impact are of less importance but nevertheless the validity of the system and the training and skills of staff inputting data should be checked.

Any inaccuracies should be corrected as soon as possible in order to limit the damage and distress caused.

Principle 5: Storage limitation

Hertford Museum will ensure that personal information is not retained any longer than is necessary. This will require Hertford Museum to undertake regular assessment and deletion. We are legally obliged to keep client files and financial records for a period of six years.

In addition, we are required to permanently retain collection donor information.

Principle 6: Integrity and Confidentiality

Hertford Museum has a duty to ensure that appropriate security measures are in place when handling personal information. This applies to both, information technology and manual files.

Individual rights

The following rights for individuals must be adhered to at all times:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Hertford Museum will always explain the purposes for processing personal data, retention periods for that personal data, and who it will be shared with. This information is contained in Hertford Museum's Privacy Notice, publically available on request and in our website. This information must be made available at the time of data collection.

Hertford Museum's privacy notice will be reviewed on an annual basis.

Hertford Museum will obtain consent for any new uses of an individual's personal data before you start the processing.

Accountability

Hertford Museum will take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.

Hertford Museum will put appropriate data protection measures in place throughout the entire lifecycle of our processing operations, maintaining documentation of our processing activities, implementing appropriate security measures

Hertford Museum will recording and, where necessary, report personal data breaches carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests

Hertford Museum has appointed a data protection officer who will ensure adhering to relevant codes of conduct.

Hertford Museum will review and update our accountability measures on an annual basis.

Glossary

Data: means information in a form in which it can be processed (automatically)

Personal data: means data relating to a living individual who can be identified either from the data, or from the data in conjunction with other information in the possession of the data controller

Data controller: is a person who, either alone or with others, controls the contents and use of personal data

Data processor: is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment

Data subject: the individual person who is the subject of any relevant personal data (information)

A personal data-filing system: any structured set of personal data accessible according to specific criteria whether centralised, decentralised or dispersed on a functional or geographical basis

Third party: someone other than the data subject, controller, processor and persons with authority of the controller or processor to process the data

Recipient: is the person to whom data is disclosed. This would include employees. The data subject has to be informed of the recipients of the data.

Data subject's consent: means any freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data to him/her being processed. Consent requires a positive opt-in, a very clear and specific statement of consent. It must be possible to withdraw consent. Consent must not be precondition of a service.