Charles
Dickens
Museum

DATA MANAGEMENT POLICY

The Charles Dickens Museum Limited acting as the sole trustee of The Dickens House and the Dickens House Fund.

This Policy was reviewed by the Board in March 2022.

1. Context and overview

1.1. Introduction

The Charles Dickens Museum (CDM) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

1.2. Why this policy exists:

This data management policy is intended for use by all employees and ensures CDM:

- complies with data protection law and follows good practice;
- protects the rights of customers, staff and partners;
- is transparent about how it stores and processes individuals' data;
- protects itself from the risks of a data breach.

1.3. Policy Statement

CDM is committed to:

- protecting the personal data of individuals from unintended loss, destruction, damage, modification, disclosure or other security risk; and

- processing the personal data of individuals fairly and lawfully in accordance with current data protection legislation.

1.4. Data protection law

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes;

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;

- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

1.5. Definitions

Data Protection legislation has a language of its own. Some helpful definitions are set out below to assist in understanding this Policy:

a) Data Controller: means a person or company who decides the purposes for which and the way in which personal data is processed. CDM is the Data Controller in respect of personal data.

b) Personal Data: means information that relates to a living person who can be identified by that information or by that information together with other information that the Data Controller has or is likely to obtain which:

- affects that person's privacy;

- is biographical of that person to a significant degree;

- has that person as its focus (as opposed to something else like a business transaction where the employee's involvement is incidental).

c) Data Subject: every living individual who is connected to CDM.

Other definitions are set out in the body of the text where appropriate.

2. Who? People and responsibilities

Everyone at CDM contributes to compliance with GDPR and needs to be aware of their respective roles and responsibilities.

CDM is the data controller and all staff are involved in aspects of data processing. Although CDM is not required to formally appoint a Data Protection Officer, the Director will assume overall responsibility, reporting to the Board and keeping the Board updated about data protection issues, risks and responsibilities.

All employees must become familiar with the aims of this policy and follow the guidelines set out. In particular, they must:

- seek advice from the Director where they have any doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with GDPR;

- not use personal information that they hold in the course of their employment for any reason other than the performance of their employment duties;

- provide assistance to the Director in the conduct of any audit or preparing a response to a subject access request;

- keep all information that they process safe and secure in accordance with any procedures issued by CDM. Where no procedures are set out explicitly, they should exercise a degree of care over the personal data that they process by considering the harm that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Director;

- not keep duplicate records where a centralised filing option is available. Duplication can complicate the process of responding to subject access requests (see section 6);

- notify the Director immediately should they detect any potential or actual breach of the GDPR.

3. Scope of personal information to be processed

CDM processes a range of personal data relating to employees, volunteers, contractors and suppliers, visitors and customers. This includes, for example:

- employee data, including details necessary for fulfilling legal employment obligations, such as date of birth, national insurance number and home address, as well as bank details, next of kin and any relevant medical conditions;

- personal information such as name, postal address, phone number, email address, and other information that visitors, customers or supporters may volunteer as part of ticket bookings, online purchases, membership or donation forms, booking forms, e-newsletter sign-ups and visitor surveys;

- Gift Aid status;

- donor status and associated information.

Data is collected through online and paper forms and is securely stored electronically and, where relevant, in filing cabinets. We have implemented security procedures, rules and technical measures to protect the personal data that we have under our control from:

- unauthorised access;

- improper use or disclosure;

- unauthorised modification.

All our employees and data processors, who have access to, and are associated with the processing of personal data, are legally obliged to respect the confidentiality of that data.

4. Data Sharing

We do not disclose personal data to any third parties or external organisations, other than data processors carrying out work on our behalf.

Examples of such data processors would be our accountants (payroll services), delivery services for fulfilling online shop orders, and bulk email distribution services.
Any such companies are acting as approved data processors for the Charles Dickens Museum, and we retain full responsibility for your personal data. Data processors will act only on our instructions.

We may occasionally need to transfer personal data overseas, for instance to our bulk email distributor, MailChimp. Where this is necessary, this may be to countries or territories around the world.

Personal data will never be sold or passed to any third party for any other purpose.

5. Security measures

Everyone at CDM has a responsibility to ensure that personal data is processed appropriately and stored securely.

If personal data is breached, this must be reported immediately to the Director, who will consider what action needs to be taken. This may include reporting to relevant authorities.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made

unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

CDM uses CCTV cameras in what it considers to be “public” areas of its premises. The use of such CCTV cameras is notified by signage at obvious places at the entrance to the monitored areas. CDM has notified such monitoring to the Information Commissioner.

6. Subject access requests

All individuals who are the subject of data held by CDM are entitled to:

- ask what information CDM holds about them and why;
- ask how to gain access to it;
- be informed how to keep it up to date;
- be informed how CDM is meeting its data protection obligations.

Anyone can ask us if we are keeping any personal data about them and request to receive a copy of that personal data – this is called a Subject Access Request.

To make a Subject Access Request, the individual will need to provide adequate proof of identity such as a copy of their passport, birth certificate or driving licence before the request can be processed.

Subject Access Requests should be passed immediately to the Director. CDM will need to identify what personal data we hold and prepare a response to the individual, including copies of the information we hold. CDM has committed to responding within 30 days (see Privacy Policy).

7. The right to be forgotten

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as ‘the right to be forgotten’. Individuals can make a request for erasure verbally or in writing, and we must respond within one month to respond.

However, the right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- we are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we have processed the personal data unlawfully;

- we have to do it to comply with a legal obligation.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing;
- for the establishment, exercise or defence of legal claims.

8. Privacy Policy and notices

CDM aims to ensure that individuals are aware that their data is being processed, and that they understand:

- who is processing their data;
- what data is involved;
- the purpose for processing that data;
- how to exercise their rights.

To these ends CDM has a Privacy Policy setting out how personal data is used, which is available on the website and on request from info@dickensmuseum.com.

9. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. CDM details here the ongoing measures implemented to:

- maintain documentation/evidence of the privacy measures implemented and records of compliance;
- regularly test the privacy measures implemented and maintain records of the testing and outcomes;
- use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts;
- keep records showing training of employees on privacy and data protection matters.