Data Protection Policy
Royal Pavilion & Museums Trust
2020-25

1. Purpose

This policy governs the use of personal data by Royal Pavilion & Museums Trust (RPMT) in the course of its business. It outlines the expected standards of practice by those working on behalf of the Trust in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

2. Targeted Audience and Scope

This policy applies to:

- Employees of RPMT
- Trustees of RPMT
- Volunteers carrying out duties for RPMT
- Organisations commissioned by the Trust and their staff
- External collaborating partners and their staff

3. Related Trust Policies and Guidelines

- Acceptable Use of ICT Policy
- CCTV Code of Practice
- Social Media and Personal Online Communication Policy

4. Background

Royal Pavilion & Museums Trust process personal data in the course of its business, usually as a data controller. It also operates alongside a trading arm, RPMT Enterprises Ltd, and acts as a joint controller for personal data used by that company, with primary responsibility for complying with the rights of data subjects.

The Trust is committed to handling all personal information in a manner that complies with the General Data Protection Regulation and the Data Protection Act 2018. It has appointed a Data Protection Officer to monitor and advise on data protection.

Royal Pavilion & Museums Trust took on management of Brighton & Hove City Council's museum service on 1 April 2020. As such, it currently processes a significant amount of

personal data that has been transferred to it by the Council, and with standards of care that are comparable to those practised by the Council.

5. Definitions

- Personal Data – Any data relating to a living person who is directly or indirectly identifiable
- Special Category Data – data relating to a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.
- Data Controller – The organisation which either individually or jointly decides the purposes and methods of data processing.
- Data Processor – An organisation which processes data on behalf of the data controller
- Processing – Just about anything which can be done with personal data

6. General Principles / Guidelines

All organisations that handle data about living individuals must comply with data protection legislation, the purpose of which is to protect the rights of the individual (referred to as 'data subjects' under the Act) when dealing with their personal or sensitive personal information.

It is worth noting that personal data includes opinions expressed about a person or information which sets out an organisation's intentions towards them.

Personal data can only be processed where there is a legal basis for doing so.

Due to its higher level of sensitivity, special category data can only be processed where an additional legal basis for processing (as set out in Article 9 of the General Data Protection Regulation) can be met.

However, data protection is not simply a barrier to using personal information. It provides a framework to ensure that data is shared in the interest of the person whose data it is or there is a clear legal obligation for its processing.

It is not always necessary to obtain the consent of data subjects when processing data. Often the legal basis on which information is held and used by the Trust is not consent. However it is necessary to be transparent when collecting somebody's information about the purposes it will be used for and if it will be shared.

The General Data Protection Regulation has introduced the principles of Privacy by Design and Privacy by Default. When designing systems and procedures for processing personal data, the Trust will follow a principle of data minimisation, ensuring that only necessary personal data is processed for the required purpose, and only accessible by those staff or third parties who require it. For larger projects which entail the creation of new systems, the re-use of data for new purposes, or the sharing of significant amounts of personal data with other parties, the Trust will conduct a Data Privacy Impact Assessment in order to consider how the risks to personal privacy can best be controlled.

6. The Data Protection Principles

There are seven data protection principles:

- **Lawfulness, fairness and transparency:** data must be processed in ways that are lawful, treat people fairly, and should be transparent to its data subjects
- **Purpose limitation:** data must be processed for clear and specific purposes
- **Data minimisation:** only the data that is necessary for fulfilling a purpose should be processed
- **Accuracy:** data must be accurate and kept up to date where necessary
- **Storage limitation:** data should only be kept for as long as it is required, and held in a form that prevents it being identified with an individual if that meets its purpose
- **Integrity and confidentiality:** security measures should be used that prevent unauthorised processing or accidental loss or damage to data.
- **Accountability:** the data controller must be responsible for personal data and able to demonstrate compliance

7. Roles and Responsibilities

The Trust's Leadership Team is responsible for ensuring that staff operate in accordance with the contents of this policy.

The Trust has appointed a qualified Data Protection Officer (DPO) who will support compliance through advice and training, and maintain an Information Asset Register. The DPO will also co-ordinate and lead responses to requests from data subjects exerting their rights over their personal information, including subject access requests.

Staff will be required to ensure that privacy notices are provided to data subjects in the course of their work and that information sharing agreements are included in contracts or other agreements which require the processing of personal data. They will also be supported to produce Data Privacy Impact Assessments where the processing of personal data may present significant risks to data subjects.

Closed circuit television (CCTV) and body worn video (BWV) are managed by the Trust's Security Team, in accordance with this policy and a CCTV Code of Practice.

8. Training Requirements

Data protection training will be periodically offered to all staff and is a mandatory element of its induction programme.

The Trust will undertake to provide its DPO with the training and resources required for the role.

All staff are expected to read and understand this policy.

9. Risks

Royal Pavilion & Museums Trust recognises the risks associated with staff processing personal data as part of its business activities.

In the event of a breach, action may be taken against the Trust (as the Data Controller) and/or the employee responsible for the breach.

Non-compliance with this policy may result in damage or distress to individuals, financial loss, reputational damage and compromise the Trust's ability to pursue its charitable objects.

The Information Commissioners' Office (ICO) has the power to issue penalties for breaches of the Data Protection Act. They may also order the Trust to stop processing personal data where they have cause to believe there is a serious risk to personal privacy.