

TATE DATA PROTECTION POLICY

Approved by the Board of Trustees on July 2003
Date of Next Review: 2010

1 Introduction

For the purposes of this Data Protection Policy, the following terms shall have the following meanings:

“*data*” means information stored or processed by a computer and information recorded as part of a relevant filing system (which includes paper-based filing systems, card indexes and other non-electronic collections of data which are structured either by reference to individuals or so that information about an individual is easily accessible).

“*personal data*” means data about a living person who can be identified by that data.

“*data subject*” means a person who is the subject of personal data.

“*processing*” means obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing or destroying data.

2 Data Protection Principles

Tate is committed to the eight **Data Protection Principles** contained in the Data Protection Act 1998, being:

Principle One – Personal data shall be processed fairly and lawfully.

Personal data shall not be processed unless at least one of the following conditions is met:

- The data subject has given consent;
- Processing is necessary for the performance of a contract or with a view to entering into a contract;
- Processing is necessary for complying with a legal obligation;
- Processing is necessary to protect the interests of the data subject;
- Processing is necessary for the administration of justice or the administration of public functions;
- Processing is necessary for the purposes of legitimate interests pursued by the data controller, except in cases that prejudice the rights and freedom of the data subject.

Sensitive personal data shall not be processed unless at least one of the following conditions is also met:

- The data subject has given explicit consent;
- Processing is necessary to perform legal obligations imposed by law in connection with employment;

- Processing is necessary to protect the vital interests of a person in the situation where consent cannot be reasonably obtained;
- Processing is carried out for the legitimate purposes of a non-profit making body established for political, philosophical, religious or trade union activities;
- The information has already been made public by the data subject;
- Processing is necessary in connection with legal proceedings;
- Processing is necessary for the administration of justice or the administration of public functions;
- Processing is of information as to racial or ethnic origin and is necessary for equal opportunity monitoring.

Principle Two – Personal data shall be obtained only for the **purposes specified** and shall only be processed for those purposes.

Principle Three – Personal data shall be **adequate, relevant and not excessive** for the purpose for which they are processed.

Principle Four – Personal data shall be **accurate and kept up to date**.

Principle Five - Personal data shall not be **kept for longer than is necessary**.

Principle Six – Personal data shall be processed in accordance with the **rights of data subjects** under the 1998 Data Protection Act. In particular, a data subject will have the right:

- To be informed whether personal data about him or her is being processed;
- To be given a description of that data, the reason why it is being processed and the names of anyone to whom it will be disclosed;
- To be told the contents of the data and where it came from;
- Where data is to be used for the purposes of automatic evaluation the logic involved in that automated process.

Tate will have the right to ask for **proof of identification** and charge a reasonable fee.

Principle Seven – Appropriate measures shall be taken against **unauthorised processing** of personal data and against accidental loss or destruction to personal data.

Principle Eight – Personal data shall **not be transferred outside the European Economic Area** without adequate protection.

3 Responsibility for Compliance with the Data Protection Act 1998

All staff involved in processing data at Tate will be responsible for ensuring compliance with data protection legislation generally and this Data Protection Policy in particular and Tate will ensure that appropriate training and guidance is provided.

Breach of data protection legislation is a criminal offence and Tate will regard wilful or reckless breach of Tate's Data Protection Policy and published procedures as a disciplinary offence and such breaches will be subject to Tate's disciplinary procedures as set out in the Staff Handbook.

The IS Development Manager will ensure that Tate's entries on the Data Protection Register are accurate and up-to-date at all times and will ensure that Tate is kept up to date on data protection issues and legislation.

Heads of Departments will be accountable for data protection compliance in their Department and for notifying the IS Development Manager of any changes to their Department's data processing activities so that the Register can be kept up to date.

4 Information Security Policy

Internal and remote access to computerised information and host application software will be controlled by appropriate levels of password, granted to Tate staff on a "need to know" basis. Security of computer information will be provided by automated backup routines, run daily on all sites and configured according to professional best practice.

The IS Department will support Tate staff to ensure the following for information resources:

- That personal information is readily accessible to authorised individuals;
- That plans and procedures are in place for the necessary long term archiving of specific record types for purposes of access;
- That clear guidelines are established for disclosure to and consultation by legitimately interested parties of personal information stored on paper or computerised media;
- That procedures are put in place for identification and removal of inappropriate or unnecessary personal data stored on any Tate information system.

5 Data Protection Registration / Notification

Tate's IS Development Manager will be responsible for keeping Tate's registrations with the Data Protection Commissioner up-to-date and accurate. Every Head of Department will be responsible for data protection issues in that Department and for notifying the IS Development Manager of any changes to their data processing activities. The IS Development Manager will review Tate's registrations on at least an annual basis.

6 Review of Policy

Tate will review its Data Protection Policy and the purposes for which it holds personal data periodically.

7 Development and/or Modification of Information Systems

All Tate staff, consultants and contractors responsible for procuring and/or creating any new information systems or modifying existing systems will be responsible for consulting with the IS Development Manager to ensure that those systems will comply with Tate's Data Protection Policy and procedures.