

Appropriate Policy Document

Introduction

This is the “Appropriate Policy Document” that sets out how the National Portrait Gallery protects special category data and criminal offence data.

Special category data is information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purposes of identification, data concerning health, or data concerning an individual’s sex life or sexual orientation.

Criminal conviction data is information relating to criminal convictions and offences or related security measures. This includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as ‘criminal offence data’.

This document meets the requirement at paragraph 1 Schedule 1 of the Data Protection Act 2018: that a data controller has an appropriate policy document in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection. It also meets the requirement at paragraph 5 Schedule 1 of the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 of the Data Protection Act 2018.

Description of data processed

We process special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, and their membership of any trade union. We process special category data as an employer for reasons of substantial public interest for purposes of equality of opportunity or treatment monitoring, and promoting racial and ethnic diversity in the organisation.

We process criminal offence data about job applicants and our employees that is necessary to fulfil our obligations as an employer and legal obligations.

Special category data

The Gallery may process special category data under the following conditions in Part 1 and Part 2 of Schedule 1:

- Employment, social security and social protection (paragraph 1)
- Health or social care purposes (paragraph 2)
- Statutory and government purposes (paragraph 6)

- Equality of opportunity or treatment (paragraph 8)
- Racial and ethnic diversity at senior levels of organisation (paragraph 9)
- Preventing or detecting unlawful acts (paragraph 10)
- Protecting the public against dishonesty (paragraph 11)
- Regulatory requirements relating to unlawful acts and dishonesty (paragraph 12)
- Preventing fraud (paragraph 14)
- Counselling etc. (paragraph 17)
- Occupational pensions (paragraph 21)

Criminal offence data

The Gallery may process criminal offence data under the following conditions in Parts 1 and 2 of Schedule 1:

- Employment, social security and social protection (paragraph 1)
- Statutory and government purposes (paragraph 6)
- Preventing or detecting unlawful acts (paragraph 10)
- Protecting the public against dishonesty (paragraph 11)
- Regulatory requirements relating to unlawful acts and dishonesty (paragraph 12)
- Preventing fraud (paragraph 14)

Accountability

Our Senior Information Risk Owner is responsible for ensuring that the department is compliant with these principles.

We will:

- ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law

Principle (a): lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner.

We will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful

- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent

Principle (b): purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We will:

- only collect personal data for specified, explicit and legitimate purposes, and inform data subjects what those purposes are in a privacy notice
- not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

Principle (c): data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

Principle (d): accuracy

Personal data shall be accurate and, where necessary, kept up to date.

We will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

Principle (e): storage limitation

Personal data shall be 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.

We will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted, put beyond use or rendered permanently anonymous.

Principle (f): integrity and confidentiality (security)

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

We will ensure that there appropriate organisational and technical measures in place to protect personal data.

Retention and erasure

We will ensure, where special category or criminal convictions personal data is processed, that:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it, put it beyond use or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period