Table of Contents

[1. Purpose 4](#_Toc53680914)

[2. Special category data 4](#_Toc53680915)

[3. Criminal convictions and offence data 4](#_Toc53680916)

[4. Conditions for processing special category and criminal offence data 5](#_Toc53680917)

[Part 1 - Conditions relating to employment, social security and social protection 5](#_Toc53680918)

[Part 2 - Substantial Public Conditions 5](#_Toc53680919)

[Statutory etc and government purposes 5](#_Toc53680920)

[Equality of Opportunity or Treatment 5](#_Toc53680921)

[Preventing or detecting unlawful acts 5](#_Toc53680922)

[Protecting the public against dishonesty etc 5](#_Toc53680923)

[Regulatory Requirements relating to unlawful acts and dishonesty etc 5](#_Toc53680924)

[Preventing Fraud 6](#_Toc53680925)

[Safeguarding of children and individuals at risk 6](#_Toc53680926)

[Safeguarding of economic well-being of certain individuals 6](#_Toc53680927)

[Occupational pensions 6](#_Toc53680928)

[Disclosure to elected representatives 6](#_Toc53680929)

[5. Procedures for ensuring compliance with Article 5 of the GDPR 6](#_Toc53680930)

[Principle 1 - Lawful, fair and transparent 7](#_Toc53680931)

[Principle 2 - Collected for specific and legitimate purposes 7](#_Toc53680932)

[Principle 3 - Adequate and limited to what is necessary 7](#_Toc53680933)

[Principle 4 - Accurate and kept up to date 7](#_Toc53680934)

[Principle 5 - Retained for no longer than necessary 7](#_Toc53680935)

[Principle 6 - Kept secure 7](#_Toc53680936)

[Accountability principle 7](#_Toc53680937)

[6. Monitoring and review 8](#_Toc53680938)

Document control

Document Control

|  |  |
| --- | --- |
| Column heading | Column heading |
| Organisation  | Torbay Council |
| Title  | Appropriate Policy Document |
| Creator  | Head of Information Governance  |
| Approvals  | Information Governance Steering Group  |
| Distribution | Public |
| Subject  | Special category processing |
| Review Date | October 2022 |

Document Amendment History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number  | Originator  | Date  | Description |
| 1.0 | Jo Beer | 10/2020 | Policy Creation and approval |
| 1.1 | Jo Beer | 03/2021 | Update to include IAO responsibility |
|  |  |  |  |

# 1. Purpose

The Data Protection Act (DPA) 2018 outlines a requirement for organisations to have an Appropriate Policy Document in place when processing special category and criminal offence data under certain specified conditions.

This documents covers our processing of special category and criminal offence data for which all of the following conditions are met:

* When we, as a data controller, are processing personal data subject to Article's 9 or 10 of the General Data Protection Regulation (GDPR)
* When we, as a data controller are processing personal data in reliance on a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA
* That the condition listed in Parts 1, 2 or 3 of Schedule 1 includes a requirement for to have an Appropriate Policy Document.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA.

# 2. Special category data

Special category data is defined under Article 9 of the GDPR as personal data which reveals:

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Genetic data
* Biometric data for the purpose of uniquely identifying a natural person
* Data concerning health, or
* Data concerning a natural's person's sex life or sexual orientation.

# 3. Criminal convictions and offence data

Article 10 of the GDPR covers processing in relation to criminal convictions and offences or

related security measures. The DPA specifically confirms that this includes personal data relating

to the alleged commission of offences or proceedings for an offence committed or alleged to have

been committed. For the purpose of this document, this will be referred to as criminal conviction

data.

# 4. Conditions for processing special category and criminal offence data

The following categories of special category data and criminal offence data is processed by the

Council and may be processed across many different types of service for the purposes as set out

Below. The Heads of Service / Service Managers for each service area are the assigned

Information Asset Owners and are responsible for information management on a day-to-day basis

and compliance to this policy.

## Part 1 - Conditions relating to employment, social security and social protection

* Processing personal data concerning health in connection with our rights under employment law.
* Processing data relating to criminal convictions in connection under Article 10 of the GDPR in connection with our rights under employment law in relation to recruitment, discipline and dismissal

## Part 2 - Substantial Public Conditions

### Statutory etc and government purposes

* Fulfilling our obligations under UK legislation for the provision of services to our customers
* Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.

### Equality of Opportunity or Treatment

* Ensuring compliance with our obligations under legislation such as the Equality Act 2010.
* Ensuring that we fulfil our public sector equality duty when delivering our services
* Ensuring that we provide equal access to our services to all of our communities.

### Preventing or detecting unlawful acts

* Processing data concerning criminal records in order to prevent and detect unlawful acts against the Council and the community.
* Carrying out enforcement action in connection with our statutory duties.

### Protecting the public against dishonesty etc

* Processing data in connection with dishonesty, malpractice or other improper conduct in order to protect our communities.
* Carrying out enforcement action in connection with our statutory duties.
* Carrying out investigations and disciplinary actions relating to our employees.

### Regulatory Requirements relating to unlawful acts and dishonesty etc

* Processing data in connection with our enforcement obligations under UK legislation
* Assisting other authorities in connection with their regulatory requirements.

### Preventing Fraud

* Disclosure of personal data in accordance with arrangements made by an anti-fraud organisation

### Safeguarding of children and individuals at risk

* Processing of data to protect a child / young person from neglect, physical, mental or emotional harm.
* Processing of data to protect an individual's physical, mental or emotional well-being.

### Safeguarding of economic well-being of certain individuals

* Processing of data to protect the economic well-being of an individual over the age of 18, where they are less able due to physical or mental injury, illness or disability.

### Occupational pensions

* Fulfilling our obligations to provide an occupational pension scheme
* Determining benefits payable to dependents of pension scheme members

### Disclosure to elected representatives

* Assisting elected representatives such as councillors and Members of Parliament where requests for assistance / enquiries are made on behalf of their constituents.

# 5. Procedures for ensuring compliance with Article 5 of the GDPR

Article 5 of the GDPR states that personal data shall be:

* Processed lawfully, fairly and transparently
* Collected for specific and legitimate purposes and not used in a manner incompatible with those purposes
* Adequate, relevant and limited to what is necessary for the purpose
* Accurate and, where necessary, kept up to date
* Retained for no longer than necessary and
* Kept secure.

In addition the principles above, Article 5 also organisations to be responsible for and be able to

demonstrate compliance with the above (accountability principle).

Our Data Protection Policy sets out how we will comply with these principles when processing

personal data and we have a Data Protection Officer in place who assists us by monitoring our

compliance and advising on our compliance.

When processing special category data we will have the following in place to ensure compliance

with above principles:

## Principle 1 - Lawful, fair and transparent

* We will only process special category or criminal conviction data where we have a lawful basis to do so.
* We will ensure that our customers are informed as to how their personal data is being processed and how they can exercise their rights.

## Principle 2 - Collected for specific and legitimate purposes

* We will only use special category data for the purpose it was originally collected and not further use it in a manner which is incompatible with the original purpose.
* If we believe we need to use this data in a new way we will advise our customers and provide them with updated privacy information.

## Principle 3 - Adequate and limited to what is necessary

* We will not collected more data than is necessary for the purpose, for example we will not collected data about race or ethnic origin unless it is essential to have this information for the purpose.

## Principle 4 - Accurate and kept up to date

* We will ensure that special category is accurate and will put measures in place to check the accuracy of data held.
* We will update personal data as soon as practicable once we have been advised as to a change.

## Principle 5 - Retained for no longer than necessary

* We will only keep special category data in a personally identifiable form for as long as necessary in accordance with our retention schedule.
* When identifiable special category data is no longer required, but data may need to be retained for performance or statistical measures it will be pseudonymised or anonymised.

## Principle 6 - Kept secure

* Measure will be taken to ensure that special category data is kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage.
* Systems and facilities holding special category data will be subject to risk assessment and review to ensure they remain secure.

## Accountability principle

In order to demonstrate compliance, we have the following measures in place:

* Records of our processing activities
* Data protection impact assessments for new processing activities and systems holding personal data
* An independent Data Protection Officer, who is responsible for monitoring and advising on our compliance
* Internal policies and procedures relating to data protection and information security
* Information Asset Owners who are the equivalent of directors and assistant directors (members of SLT) are responsible for the day-to-day management of information within their services. They are supported by Information Asset Administrators who are officers with day-to-day handling responsibilities of information.
* Data Processing Agreements where we engage third parties to carry out processing on our behalf
* Records of incidents and data breaches, along with recommendations issued
* Information sharing agreements where personal data is shared on a routine basis with partner organisations.

# 6. Monitoring and review

This policy will be reviewed every 2 years by the Council’s Information Governance Steering Group (IGSG) to ensure that any national or local guidelines, standards or best practices that have been issued are considered and reflected in the policy.