## Data Protection Act 2018 - Appropriate Policy Document

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

This document covers the processing of special category and criminal offence data by Basingstoke and Deane Borough Council in accordance with the substantial public interest conditions set out in Schedule 1, Part 2 of the Data Protection Act 2018 and the condition for processing employment, social security and social protection data, under Schedule 1, paragraphs 1(1) (b) and 5. Such processing is required to be in compliance with the General Data Protection Regulation (GDPR) Article 5 principles.

### Description of Personal Data

The following categories of special category and criminal offence data is processed by the council for the purposes as set out:

**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 under Article 10 UK GDPR in connection with our rights under employment law in connection with recruitment, discipline or dismissal.

**Part 2 - Substantial Public Interest Conditions**

**Statutory etc. and government purposes**

- Fulfilling the Council's obligations under UK legislation for the provision of services to residents and 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 the Council's obligations under legislation such as the Equality Act 2010.
- Ensuring that we fulfil our public sector equality duty when carrying out our work.
- Ensuring we provide equal access to our services, to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.

The personal data processed under this category is limited to:

- Personal data revealing racial or ethnic origin
- Personal data revealing religious or philosophical beliefs
- Data concerning health
- Personal data concerning an individual's sexual orientation

**Racial and ethnic diversity at senior levels of organisations**

- To ensure the promotion of or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the council.

**Preventing or detecting unlawful acts**

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the Council and the community.
- Carrying out enforcement action in connection with the Council's statutory duties.

**Regulatory requirements relating to unlawful acts and dishonesty etc.**

- Complying with the Council's enforcement obligations under UK legislation.
- Assisting other authorities in connection with their regulatory requirements.

**Preventing fraud**

- Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

**Safeguarding of children and individuals at risk**

- Protecting vulnerable children and young people from neglect, physical, mental or emotional harm.
- Sharing information with relevant agencies for the purpose of safeguarding

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

- To protect the economic wellbeing of an individual at economic risk who is aged 18 or over.
- Data sharing with our partners to assist them to support individuals.

**Disclosure to elected representatives**

- Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

## Part 3 - Additional Conditions Relating to Criminal Convictions, etc.

Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.

- The council may process personal data relating to criminal convictions or offences in connection with its statutory functions or as part of recruitment and employment checks.

## Schedule 1 Condition for Processing

The processing of personal data to which this policy applies is in reliance of a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA.

The council's Record of Processing Activities set out the lawful basis under Article 6 of the GDPR for each activity.

## Procedures for securing compliance within Article 5 of the General Data Protection Regulation and Data Protection Act 2018

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

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

Our Data Protection Policy sets out requirements for the data protection principles to be complied with when processing personal data. Our Data Protection Officer ensures that the data protection principles are applied and that we can be held accountable for the personal data it processes.

When processing special category data, the following procedures are used to ensure compliance with the data protection principles:

### Principle a - lawful, fair and transparent

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We will:

- ensure that personal data is only processed where a lawful basis applies
- ensure lawful bases are set out within our Records of Processing Activities for each service area
- ensure that data subjects are provided with privacy notices when their data is collected

**Principle b - collected for specific and legitimate purposes**

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 we will 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 - adequate, relevant and limited to what is necessary**

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 ask for the minimum personal data that we need for the purpose for which it is collected
- ensure that the data we collect is adequate and relevant.

**Principle d - accurate and, where necessary, kept up-to-date**

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
- take particular care to do this where our use of the personal data has a significant impact on individuals.

**Principle e - retained for no longer than necessary**

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 or rendered permanently anonymous
- set out in our retention schedule and Records of Processing Activities how long information will be kept for

**Principle f - keep secure**

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
- adhere to the Government's Minimum Cyber Security Standards and implements information security controls in line with Public Sector Network (PSN) and Payment Card Industry
- ensure regular meetings of our Information Governance Strategy Group to provide suitable information security governance is deployed throughout the council
- ensure all staff who require access to information over the PSN are vetted in line with HMG Baseline Personnel Security Standard
- provide annual data protection training to all staff
- employ technical security controls to secure sensitive information within systems
- implement role based access controls to restrict access to sensitive data

**Accountability principle**

In order to demonstrate compliance with the Accountability Principle, We have implemented the following measures we:

- keep a record of all our personal data processing activities
- carry out Data Protection Impact Assessments where required
- have appointed a Data Protection Officer
- have in place internal policies and procedures for data protection and information security
- undertake regular data protection audits
- ensure suitable contracts are in place in respect of third party processing of personal data
- maintain records of security incidents, data protection rights requests and information sharing with partner agencies

**Retention and destruction of personal data**
Personal data is held and disposed of in line with the council's Retention and

Disposal Schedule. When disposing of information, we make sue this is carried out securely by using physical destruction methods as well as electronic data deletion. Disposal of information in line with our Retention Schedule is recorded on our disposal log.

Our Records of Processing Activities contain details of the retention periods for all personal data held by our service areas, together with information on the lawful basis for processing this data. If information is not retained or deleted in line with the policy then the reason is recorded.

**Responsibility for the processing of special category and criminal data**

All employees are required to comply with our Information Governance Policies when processing personal data and to ensure that any processing of the personal data is carried out legally, fairly and transparently.

**Appropriate Policy Document Review**

This document will be reviewed on an annual basis in April each year.