Appropriate Policy Document

Date of Publication:
Version:1.0

Table of Contents

1. Introduction

This is the 'Appropriate Policy Document' for Birmingham City Council (BCC) that explains the requirements the Council will meet when processing personal data relating to criminal offences (including the suspected and alleged commission of offences) and how staff can comply with these requirements when carrying out their work.

It explains the data protection regime that applies when processing personal data for law enforcement purposes. It covers part 3 of the Data Protection Act 2018 (DPA 2018), which implements an EU Directive (Directive 2016/680) and is separate from the GDPR regime.

This policy also covers the processing of special category data and criminal convictions and offences data in section, article 9 and 10 of the GDPR.

Definitions:

Law enforcement purpose – the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This definition includes the alleged commission of criminal offences by the data subject.

Special category data is defined at Article 9 GDPR as personal data revealing: Racial or ethnic origin; Political opinions; Religious or philosophical belief; Trade union membership; Genetic data; Biometric data for the purpose of uniquely identifying a natural person; ; Data concerning health; Data concerning a natural person's sex life or sexual orientation.

Article 10 GDPR deals with the processing of personal data relating to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 states that such processing also includes the processing of 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 in this document as 'criminal data'.

Schedule 1 to the DPA 2018 provides conditions for processing special category and criminal offence data and some of these conditions require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles relating to the processing of personal data in Article 5 of the GDPR and our policies regarding the retention and erasure of such personal data.

2. Conditions for processing special category and criminal data

We process special categories of personal data under the following paragraphs of Article 9 GDPR. Where appropriate we have set out the

conditions in Schedule 1 to the DPA 2018, which we use to legitimise our processing. Except where specified, processing requires an APD:

- Article 9(2)(a) – explicit consent.

Where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or the data subject in connection with employment, social security or social protection.

For these purposes, we rely on the condition at Schedule 1 paragraph 1 to the DPA 2018 to legitimise this processing.

- [Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

For these purposes, we do not need a condition under Schedule 1 to the DPA 2018, nor do we need an appropriate policy document.]

- Article 9(2)(f) – where processing is necessary for the establishment, exercise or defence of legal claims.

For these purposes, we do not need a condition under Schedule 1 to the DPA 2018, nor do we need an appropriate policy document.

- Article 9(2)(g) - where processing is necessary for reasons of substantial public interest.

For these purposes, we rely on the conditions set out in Schedule 1 Part 2 to the DPA 2018, for legitimising this processing.

- Article 9(2)(h) - where processing is necessary for health or social care purposes

For these purposes, we rely on the condition at Schedule 1 Part 1 paragraph 2 to the DPA 2018 to legitimise this processing.

- [Article 9(2)(i) - where processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

For these purposes, we rely on the condition at Schedule 1 Part 1 paragraph 2 to the DPA 2018 to legitimise this processing.]

- Article 9(2)(j) – where processing is necessary for archiving purposes in the public interest.

For these purposes, we rely on the condition set out in Schedule 1 Part 1 paragraph 4 to the DPA 2018.

We also process criminal offence data under Article 10 of the UK GDPR. For these purposes, we rely on the conditions as appropriate in Schedule 1 Part 3 to the DPA 2018.

3.Law Enforcement Processing

The GDPR expressly does not apply to the processing of personal information by competent authorities for law enforcement purposes but is covered in the UK by part 3 of the DPA 2018.

The Data Protection Act 2018 Part 3 only applies to 'competent authorities' that are processing personal data for the primary purpose of law enforcement. It applies, but is not limited, to:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

This therefore includes the Council when it undertakes a function or exercises a power in relation to the prevention, investigation, detection or prosecution of criminal offences.

Specifically, ‘law enforcement processing’ captures the processing by a competent authority of criminal offence and criminal penalty data wholly or partly by automated means or if the data forms, or is intended to form, part of a filing system.

Key law enforcement data processing provisions Part 3 of the Act strengthens the rights of data subjects whilst enabling a controller to restrict these rights where this is necessary to, amongst other things, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences, for example by revealing to a person that they are under investigation.

This Part sets out six data protection principles which apply to law enforcement processing by a competent authority. The requirements are that:

processing be lawful and fair;
the purposes of processing be specified, explicit and legitimate;
personal data be adequate, relevant and not excessive;
personal data be accurate and kept up to date;
personal data be kept no longer than is necessary; and
personal data be processed in a secure manner.

Sets out the rights of individuals over their data. These include:

rights of access by the data subject to information about the data processing (including the legal basis for processing, the type of data held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint);
the right to rectification of inaccurate data and of erasure of data (or the restriction of its processing) where the processing of the data would infringe the data protection principles; and
rights in relation to automated decision-making (that is, decision making that has not involved human intervention).

Places restrictions on those rights, but only where necessary and proportionate in order to:

avoid obstructing an investigation or enquiry;
avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
protect public security;
protect national security; and
protect the rights and freedoms of others

We have appointed a Data Protection Officer to provide independent advice and monitoring of BCC's personal data handling and that this person has access to report to the highest management level of BCC.

Compliance with the accountability principle

In accordance with the accountability principle, BCC maintains records of its law enforcement processing activities under section 61 DPA 2018. These records include information about whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, the condition in Schedule 8 which is relied on, how the processing satisfies section 35 (lawfulness of processing), and whether the personal data is retained and erased in accordance with its retention and erasure policies and, if it is not, the reasons for not following those policies.

4.Version Control

Version	Date	Notes
1.0	July 2021	

4.1 5. Points of contact for this policy

The Corporate Information Governance Team can be contacted by email or in writing at the following address:

Corporate Information Governance Team
Third Floor, 10 Woodcock Street
Birmingham
B2 2YY

infogovernance@birmingham.gov.uk