Appropriate Policy Document

This is the Appropriate Policy Document (APD) for Nottingham City Council setting out how we will protect Special Categories of Data and Criminal Offence Data.

This document supports Nottingham City Council's Data Protection Policy, and meets the requirement of the Data Protection Act 2018 (DPA 2018) that an APD be in place where processing Special Categories of Data and Criminal Offence Data in certain circumstances.

Description of Data

Nottingham City Council process the following types of Special Category Data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; data concerning health (both physical and mental health); data concerning sex life or sexual orientation.

The Council also processes Criminal Offence Data. This includes personal data relating to criminal convictions, (alleged) offences, (alleged) commission of offences, related security measures, proceedings for an offence committed or alleged to have been committed, including sentencing. Collectively this is referred to as 'Criminal Offence Data'.

Conditions for Processing

Nottingham City Council processes Special Category and Criminal Offence Data for the following purposes under Schedule 1 of the Data Protection Act 2018:

Part 1:

- §1 - employment and social protection
- §2 - health or social care purposes
- §6 - statutory purposes

Part 2:

- §8 - equality of opportunity
- §9 - racial and ethnic diversity at senior levels of organisations
- §10 - preventing or detecting unlawful acts
- §12 - regulatory requirements relating to unlawful acts and dishonesty
- §14 - preventing fraud
- §17 - counselling, etc
- §18 - safeguarding of children and of individuals at risk

- §19 - disclosure to elected representatives
- §20 - insurance
- §21 - occupational pensions

Part 3:

- §28 - extension of Part 2 conditions to cover Criminal Offence Data

Procedures for ensuring compliance with the principles

The UK General Data Protection Regulation (UK GDPR) requires personal data to be processed in accordance with the Data Protection Principles set out in Article 5(1). Article 5(2) requires Controllers to be able to demonstrate compliance with Article 5(1). The Council complies with the Principles which require Personal Data to be:

A. **Processed lawfully, fairly and in a transparent manner**. We are open and transparent when we collect Special Category or Criminal Offence Data. We do this by making detailed Privacy Notices providing clear information to individuals about why we process their personal data, and we only use the data for the reasons specified in the Privacy Notices. We process Special Category and Criminal Offence Data under the lawful bases set out in Articles 6, 9 and 10 of the UK GDPR and, where required, when we have identified a condition under Schedule 1 of the DPA 2018.

B. **Collected only for specified, explicit and legitimate purposes** and not use it for purposes that are incompatible with the purposes it was originally collected for. We only process Special Category and Criminal Offence Data where we have a lawful basis to do so.

C. **Adequate, relevant and limited to what is necessary.** We process sufficient data that is directly connected to us fulfilling our stated purposes. We do not collect excessive data beyond our purposes. Data that is no longer required at the end of its retention period will be securely destructed/deleted or rendered permanently anonymous.

D. **Accurate and where necessary kept up to date**. The Council undertakes Information Asset Audits to identify data which is inaccurate or out of date. Following the audit, data that requires updating, anonymising, or destructing/deleting is dealt with without delay. Further to this Data Subjects can exercise their Right to Rectification to request that the Council update and rectify any incorrect data held about them.

E. **Not kept in a form which identifies Data Subjects for longer than is necessary** for the purposes for which the data is processed, and once we no longer need the data, it will be deleted or rendered permanently anonymous.

F. Processed in a manner that ensures its **security using appropriate technical and organisational measures** to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. Our Information Technology (IT) Specialists together with the Data Protection Officer analyse the risks presented by our processing and to ensure that the appropriate level of security is maintained. Security mitigations include multi-factor authentication and encryption.

In addition to these Principles the Council is responsible for and must be able to demonstrate compliance with the Accountability Principle.

Accountability

We have put in place appropriate technical and organisational measures to meet the requirements of accountability and protect personal data. The Council have appointed a Data Protection Officer (DPO) whose role and responsibilities align with the provisions of Articles 37-39 of the UK GDPR. The DPO provides independent advice and monitoring of the Council's personal data handling.

In addition to this our Information Asset Register sets out the personal data categories we process, the purposes, the lawful bases under Article 6 and Article 9 of the UK GDPR including the Schedule 1 of the DPA 2018 condition as well as our retention periods for the data, recipients of personal data, international transfers of data and our means of keeping data secure.

Further to this the Council publishes Privacy Notices on our public website to explain to individuals how and why their data is processed by the Council, what their rights are, and how they can get in touch with our DPO and the Information Commissioner.

Where required, the Council enters into appropriate written arrangements with other Controllers, Joint Controllers and Processors in accordance with Articles 26 and 28 of the UK GDPR to ensure that personal data is processed lawfully and securely. The Council fully endorses and adheres to the Data Protection Principles set out in Article 5 of the UK GDPR and demonstrates compliance with the Principles through a suite of Policies and Guidance documents, including the Data Protection Policy, Records Management Policy, Data Breach Guidance, Personal Information Request Guidance, and IT Acceptable Use Policy.

In addition, the Council also undertakes Data Protection Impact Assessments (DPIAs) to assess if the use of personal data is likely to result in a high risk to individuals' interests and implement appropriate security measures which are proportionate to the risks associated with the processing.

Retention and Erasure Policies

Our Information Asset Register categorises types of data and lists the legislation that provides the retention period for that category of data. All data logged on the register is categorised and therefore the retention period for that data is known at the outset. Further information is available in the Council's Records Management Policy and Retention and Disposal Schedule. For Paper Records that are kept in an off-site storage facility, the retention periods are clearly marked on our system with Special Category and Criminal Offence Data securely destroyed once retention periods have expired unless there are lawful reasons for the data to be kept.

APD review date

October 2028

Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
1.2	Update to definition of Criminal Offence Data. Streamlining and shortening of information under the 'Principles' section.	Deputy DPO	21/10/2026	06/11/2026

Contact

Data Protection Officer
Loxley House, Station Street, Nottingham, NG2 3NG
data.protectionofficer@nottinghamcity.gov.uk