Law Enforcement Processing: Part 3 of the Data Protection Act 2018 Appropriate Policy Document

Version	Status	Date	Next Review Date
V1.0	Published	March 2021	March 2023

Sensitive processing for law enforcement purposes

As part of the Council's statutory functions, we can investigate and prosecute individuals and organisations for certain offences including Trading Standard offences, school non-attendance offences, blue badge fraud offences, planning and highway offences. The Council is a competent authority for the purpose of section 30 (1) (b) of Part 3 of the Data Protection Act 2018 (DPA 2018) which applies to authorities that have legal powers to process personal data for law enforcement purposes.

These purposes are set out at section 31 DPA 2018 and include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which might include the safeguarding against and the prevention of threats to public security.

Sensitive processing

Part 3 of the DPA 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to UK GDPR special category data. Sensitive processing means:

- the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- the processing of data concerning health;
- the processing of data concerning an individual's sex life or sexual orientation.

This policy document

This policy document outlines our sensitive processing for law enforcement purposes and explains:

i) Our procedures for securing compliance with the law enforcement data protection principles;

ii) Our policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

This document should be read alongside the Council's Data Protection Policy .

Description of data processed

We carry out sensitive processing for law enforcement purposes in the following areas:

- i) Criminal investigations
- ii) Prosecutions
- iii) Prevention or detection of criminal offences

Consent or Schedule 8 condition for processing

We carry out sensitive processing under section 35(3) DPA 2018 only in reliance on the consent of the data subject or where it is strictly necessary for the law enforcement purposes and it meets one of the following conditions in schedule 8 of the DPA 2018.

1. Statutory etc purposes
2. Administration of justice
3. Protecting individual's vital interests
4. Safeguarding of children and of individuals at risk
5. Personal data already in the public domain
6. Legal claims
7. Judicial acts
8. Preventing fraud
9. Archiving etc

The condition which will be most relevant to the Council's processing will be statutory purposes which will apply where the processing is necessary for the exercise of a function conferred on the Council by legislation and is necessary for reasons of substantial public interest.

Procedures for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.

- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high risk processing.
- We regularly review our accountability measures and update or amend them when required.

Principle (1): lawfulness and fairness

Processing for law enforcement must be lawful and fair. Sensitive processing is only permissible if it is:

based on the consent of the data subject - section 35(4);

or

is strictly necessary for the law enforcement purpose and is based on a Schedule 8 condition - section 35(5).

Our processing of sensitive data for law enforcement purposes satisfies the first Schedule 8 condition that it is necessary for the exercise of a function conferred on the Council by the legislation which provides us with law enforcement powers and is necessary for reasons of substantial public interest. We have powers under the law to prevent, detect, investigate and prosecute offences relating to our functions. The Council working to ensure offences relating to our functions are investigated and prosecuted is of substantial public interest.

In circumstances where we seek consent, we make sure consent is:

- unambiguous
- given by an affirmative action
- recorded as the condition for processing

Principle (2): purpose limitation

We process personal data for the law enforcement purposes including the prevention, investigation, detection or prosecution of criminal offences.

We are authorised by law to carry out sensitive processing for any of these purposes. We may process personal data collected for one of these purposes (whether by us or another controller), for any of our other law enforcement purposes providing the processing is necessary and proportionate to that purpose.

We will only use data collected for a law enforcement purpose for purposes other than law enforcement where we are authorised by law to do so.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

Principle (3): data minimisation

We do not systematically collect sensitive personal data for law enforcement purposes. The information we process is necessary for and proportionate to our

purposes. It is processed in the context of us carrying out processes which enable us to meet our stated purposes for processing.

Principle (4): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, we will document our decision.

We distinguish between personal data based on facts and personal data based on personal assessments or opinions and mark the file to reflect the distinction where we can. There are circumstances where this is not possible.

Where relevant, and as far as possible, we distinguish between personal data relating to different categories of data subject, such as

- People suspected of committing an offence or being about to commit an offence
- People convicted of a criminal offence
- Known or suspected victims of a criminal offence
- Witnesses or other people with information about offences

We only do this where the personal data is relevant to the purpose being pursued.

We do this by marking the file in our records. Should the status of a data subject change, our systems allow us to note the reason and amend the file.

We take reasonable steps to ensure that personal data which is inaccurate, incomplete or out of date is not transmitted or made available for any of the law enforcement purposes. We do this by checking any data before sending it externally. We also provide the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data.

If we discover, after transmission that the data was incorrect or should not have been transmitted, we will tell the recipient as soon as possible.

We document our decision to make personal data available for any of the law enforcement purposes.

Principle (5): storage limitation

All sensitive personal data processed by us for law enforcement purposes is retained for the periods set out in the Council's retention schedules. We determine the retention periods for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedules are reviewed regularly and updated when necessary.

Principle (6): security

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises and is processed where necessary by staff working away from our offices in line with relevant policies and procedures. Where it

is necessary for us to share information with third parties we consider the technical or organisational security measures they have in place before allowing access or transmitting data.

Electronic and hard copy information processed for the law enforcement purposes is only available to staff who carry out the processing for these purposes. Our electronic systems and physical storage have appropriate access controls applied.

Retention and erasure policies

We have retention schedules which include personal information processed for law enforcement purposes. Our electronic data management system includes the facility to automatically delete documents once the retention period has ended.

Our retention and erasure practices are set out in our retention schedules which are available on request.

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed every two years or revised more frequently if necessary.

Note: The County Council also has a Schedule 1, Part 4, Data Protection Act 2018 Appropriate Policy Document which covers processing special category data and criminal offence data based on the Schedule 1 substantial public interest conditions and employment, social security and social protection condition.