Safeguarding use of personal data when meeting the Council's law enforcement responsibilities

As part of Hertfordshire County Council's statutory functions we may investigate and prosecute organisations and individuals who commit offences under a wide range of legislation, including but not limited to, our youth justice functions; school attendance, child employment and performance licences; consumer protection; business regulation; fraud against the council; and environmental protection including waste disposal.
We may also investigate in matters relating to the protection of children or vulnerable adults in furtherance of our statutory powers.

Where we have enforcement powers we are considered to be a competent authority for the purpose of Part 3 of the Data Protection Act (DPA) 2018 which applies to the processing of personal data by such authorities for law enforcement purposes. The Law enforcement purposes are set out at Section 31 DPA 2018 and include the prevention, investigation, detection, or prosecution of criminal offences.

We are also able to carry out ***Sensitive processing*** in accordance with the conditions of Schedule 8 of the DPA 2018. Sensitive processing is defined at s. 35 (8) as:

- 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

For the purpose of this policy we carry out sensitive processing only where it is strictly necessary for the law enforcement purposes or in the substantial public interest or where we have the consent of the data subject.
This document forms our policy to ensure that appropriate safeguards are in place when sensitive data is processed as required by paragraph 39 of part 4 of Schedule 1 and S 35 (4) (b) of the DPA 2018.

Section 35 - First data protection principle *lawful and fair*

Processing for law enforcement purposes must be lawful and fair. It is only lawful if, and to the extent that,

- it is based on law and
- either the data subject has given their consent for the processing
- or the processing is necessary for the law enforcement purpose
- or the processing meets at least one of the conditions in Schedule 8.

Our processing for law enforcement purposes satisfies the first Schedule 8 condition, that it is necessary for the exercise of the functions conferred on the Council by legislation and is necessary for reasons of substantial public interest. We are required to seek to prevent, detect, investigate and prosecute possible offences in relation to our responsibilities.

This policy will be reviewed every two years or revised between reviews where it becomes necessary.

In circumstances where we seek consent, we make sure

- The consent is clear
- The consent is given by an affirmative action
- The consent is recorded as the condition for processing

Section 36 – Second data protection principle *specified purpose*

We process personal data for all of the law enforcement purposes listed at section 31 DPA 2018. These are 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. The offences relate to our youth justice functions; school attendance, child employment and performance licences; consumer protection; business regulation; fraud against the council and environmental protection including waste disposal.

We are authorised by law to process personal data 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 the law allows us to.

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

Section 37 – Third data protection principle *adequate, relevant and not excessive*

We do not systematically collect sensitive personal data for law enforcement purposes. Our processing is necessary for, and proportionate to, our purposes. Personal data is only processed to enable us to meet our stated purposes.
Where sensitive personal data is provided to us or obtained by us but is not relevant to our stated purposes, we will erase it.

Section 38 – Fourth data protection principle *accurate and up to date*

Where we become aware that personal data is inaccurate or out of date, 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 will seek to distinguish between personal data relating to different categories of data subject, such as

- People suspected of committing an offence or being about to commit and 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.

This policy will be reviewed every two years or revised between reviews where it becomes necessary.

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 verifying any data before sending it externally.

Section 39 – Fifth data protection principle *kept for no longer than necessary*

We have a retention schedule for information held by the Council and retain personal data processed for the purposes of law enforcement for 6 years from closure of the matter unless there is a legitimate reason to retain it for longer.

Section 40 – Sixth data protection principle *appropriate security*

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises.

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.
The systems we use to process personal data for law enforcement purposes allow us to erase or update personal data at any point in time. They also allow us to log the following information:

- Collection
- Alteration
- Consultation (access)
- Identity of person who accessed
- Disclosures
- Combination of records
- Erasure

Safeguards in respect of archiving

Where personal data is retained as a public record to be transferred to Hertfordshire Archives and Local Studies as the official Place of Deposit, our condition for processing is the last Schedule 8 condition – that the processing is necessary for archiving purposes in the public interest.

Automated Decision-Making safeguards

The Council does not make automated decisions in respect of law enforcement processing.

This policy will be reviewed every two years or revised between reviews where it becomes necessary.