Policy on processing special categories of personal data and criminal convictions data

Personal data is not all the same, and some information is more sensitive than others. As such special rules apply when processing these 'special categories' of personal data. This special category processing policy should be read alongside Harrow Council's Privacy Information Notice.

This is the appropriate policy document for Harrow Council that sets out how we will protect special category and criminal convictions personal data.

This policy meets the following requirements of the Data Protection Act 2018, specifically:

- Paragraph 1 of Schedule 1 requiring that an appropriate policy document be in place where the processing of special category personal information necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection

- Paragraph 5 of Schedule 1 requiring that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act.

- Section 42 requiring that an appropriate policy document is in place in respect of processing of personal information for law enforcement purposes

Special categories' of personal data include:

- Racial or ethnic origin;
- Political opinions;
- Religious and philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person; and
- Sex life/sexual orientation.

The processing of criminal offence data also has additional legal safeguards. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

The Council can process special category data where:

- The data subject consents to the processing.
- The processing is necessary for:
  - carrying out our rights in the field of employment law, social security, and social protection;
  - protecting the vital interests of the data subject when we cannot obtain consent;
  - establishing, exercising, or defending legal claims;
  - reasons of substantial public interest;

Article 5 of the General Data Protection Regulation sets out the data protection principles. This policy addresses each principle and explains how we satisfy the requirements:

Principle 1

- 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, and where processing is otherwise lawful only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing ensure that data subjects receive full privacy information so that any processing of personal data is transparent

Principle 2

- 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. We will 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 you first.

Principle 3

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

Principle 4

- 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. We take every reasonable step to ensure that your personal data is accurate and erase or rectify without delay when we are notified of errors.

Principle 5

- 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.

Principle 6

- 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 ensure that there are suitable privacy policies and keep sufficient records of our processing activities. We have strong technical measures in place to protect personal data. See security principle below.

Accountability principle

- The controller shall be responsible for, and be able to demonstrate compliance with these principles. Our Data Protection Officer is responsible for monitoring our compliance with these principles.

We will ensure that records are kept of all personal data processing activities and the envisaged time limits for erasure of the different categories of data. We carry out Data Protection Impact Assessments for any high risk personal data processing, and consult the Information Commissioner if appropriate. We have appointed a Data Protection Officer (DPO) who provides independent advice and monitoring of the departments' personal data handling. Our DPO reports to the highest management level of the council. We have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law

We will ensure, where special category or criminal convictions personal data is processed, that:

- there is a record of that processing, and that record will set out, where possible, where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

How do we protect your information?

We will do what we can to make sure we hold personal records about you (paper and electronic) in a secure way and we will only make them available to those who have a right to see them. Examples of our security processes include:

- Encryption – meaning that information is hidden so that it cannot be read without special knowledge (such as a password).
- Pseudonymisation – meaning that we will use a different name so we can hide parts of your personal information from view. This means that someone outside of the Council could work on your information for us without ever knowing it was you.
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it.
- Training our staff to make them aware of how to handle personal information and how and when to report when something goes wrong.
- Regular testing of technology and upgrading security measures including keeping up to date on the latest security updates (commonly called "patches")

For further information about Harrow Council's compliance with data protection law, please contact us: DPO@harrow.gov.uk