Special category data policy

As part of our statutory and corporate functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

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 covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes 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 as 'criminal offence data'.

Schedule 1 of 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 policies regarding the retention and erasure of such personal data.

Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018 and is the subject of a separate document.

Conditions for processing special category and criminal offence data
We process special categories of personal data under the following GDPR Articles:

- 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
- Article 9(2)(g) - reasons of substantial public interest. We are responsible for waste disposal and strategic planning. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role
- Article 9(2)(i) - for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health
- Article 9(2)(j) - for archiving purposes in the public interest. The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 - archiving

- Article 9(2)(f) - for the establishment, exercise or defence of legal claims
- Article 9(2)(a) - explicit consent. In circumstances 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)(c) - where processing is necessary to protect the vital interests of the data subject or of another natural person

We also process criminal offence data under Article 10 of the GDPR.

Procedures for securing compliance with the principles in Article 5 of the GDPR
Article 5 of the GDPR sets out the data protection principles. These are our procedures for ensuring that we comply with them.

First principle
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

Second principle
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
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we use personal data for a new purpose that is compatible, we will inform the data subject first

Third principle
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.

Fourth principle
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 will take particular care to do this where our use of the personal data has a significant impact on individuals.

Fifth principle
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. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary. (For more information see the paragraph on the retention and erasure of personal data below.)

Sixth principle
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 will ensure that there appropriate organisational and technical measures in place to protect personal data for example:

- Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures
- Our electronic systems and physical storage have appropriate access controls applied
- The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate

Accountability principle
The GDPR states that the data controller must be responsible for, and be able to demonstrate, compliance with these principles. Our Senior Information Risk Officer and Caldicott Guardians (for social care personal data) are responsible for ensuring that the department is compliant with these principles.

We will:

- Ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request
- Carry out a Data Protection Impact Assessment for any high risk personal data processing and consult the Information Commissioner if appropriate
- Appoint a Data Protection Officer to provide independent advice and monitoring of the departments' personal data handling and that this person has access to report to the highest management level of the department
- 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 legislation

Data controller's policies regarding retention and erasure of personal data
We will ensure, where special category personal data or criminal offences data are processed, that:

- There is a record of that processing and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- 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
- 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
- We retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements

To work out the right retention period for personal data, we consider the following matters:

- The amount, nature, and sensitivity of the personal data
- The potential risk of harm from unauthorised use or disclosure of personal data
- The purposes for which we process your personal data and whether we can achieve those purposes through other means and
- Any legal or regulatory requirements

Once services are no longer required from us by a person, we will retain and securely destroy their personal information in accordance with our data retention schedule.

Your rights
The General Data Protection Regulation gives you a number of rights in relation to your personal data:

- Right to access a copy of your personal data.
- Right to have your personal data corrected.
- Right to have your personal data deleted (“right to be forgotten”).
- Right to restrict how we use your personal data.
- Right to ask us to transfer your personal data to another service provider.

You can get more information about these rights in the Council’s Privacy Policy.

If you wish to exercise any of these rights please contact our Information Governance team on informationgovernance@rother.gov.uk in writing or by completing our online form.

If you are dissatisfied with how we have used your personal data you have a right

to complain to the Information Commissioner's Office at casework@ico.org.uk.

Identity of Data Protection Officer
If you have any questions or concerns about how your personal data is handled, you can contact our Data Protection Officer (DPO), Graham McCallum, at dataprotection@rother.gov.uk