

East Hertfordshire District Council - Appropriate Policy Document

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require East Hertfordshire District Council ('the Council') to have an APD in place.

This document serves as the Council's APD and demonstrates that the processing of SC and CO data based on the specific Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles.

1. Description of data processed

As noted in the Council's Article 30 Record of Processing Activity (ROPA), the following categories of SC and CO data are currently processed:

- Data concerning health;
- Personal data revealing racial or ethnic origin;
- Data concerning sexual orientation (staff only);
- Personal data revealing trade union membership (staff only);
- Data concerning criminal convictions;
- SC and/or CO data captured through the Council's use of surveillance technologies and;
- Data concerning criminal allegations.

2. Schedule 1 conditions for processing

Where required, the Council relies on the following DPA 2018 Schedule 1 conditions for processing SC and CO data:

- (1) – Employment, social security and social protection;
- (3) – Public Health;
- (2) – Health or social care purposes;
- (6) – Statutory and government purposes;
- (10) – Preventing or detecting unlawful acts and;

- (18) – Safeguarding of children and individuals at risk.

3. Procedures for ensuring compliance with the principles

The Council shall be responsible for, and shall be able to demonstrate, compliance with the UK GDPR principles. The Council's Information Governance and Data Protection Manager is our Data Protection Officer and supports us in complying with these principles. For more information on how the Council processes your general personal data, please see our [corporate privacy notice](#).

In order to ensure that the Council complies with the principles in the UK GDPR when processing your SC and CO data and only processes this data under the conditions in section 2 above; we currently implement the procedures below:

Accountability principle
<p>The Council will:</p> <ul style="list-style-type: none"> • Maintain appropriate documentation of our processing activities and information assets and will make these available to the Information Commissioner upon request. • Implement and review appropriate data protection policies and procedures to ensure that SC and CO data is only collected, used or handled in a way that complies with data protection law. • Carry out a Data Protection Impact Assessment for any high risk processing, and consult the Information Commissioner if appropriate. • Ensure the Data Protection Officer is appointed to provide independent advice and monitoring of our services' SC and CO data handling, and that this person reports to the highest levels of the Council.
Principle (a): lawfulness, fairness and transparency
<p>The Council will ensure that:</p> <ul style="list-style-type: none"> • Where we process SC and CO data, that in addition to an article 6 (UK GDPR) lawful basis, a Schedule 1 (DPA 2018) condition for processing applies. This information will be recorded in the Council's ROPA and in this APD. • We are open and honest when collecting SC and CO data and that you are not misled about its use. • We make appropriate privacy information available with respect to SC and CO data. This will be done using an appropriate privacy notice.
Principle (b): purpose limitation
<p>The Council will:</p> <ul style="list-style-type: none"> • Ensure that we have identified purposes for processing SC and CO data and that this data is only collected and processed for these specified, explicit and legitimate

Accountability principle
<p>purposes. We will inform you of these purposes in an appropriate privacy notice.</p> <ul style="list-style-type: none"> • Not use SC and CO data for purposes that are incompatible with the purposes for which it was collected unless we have consent. If we do use this data for a new purpose that is compatible, we will inform you about this first.
Principle (c): data minimisation
<p>The Council will:</p> <ul style="list-style-type: none"> • Only collect the minimum amount of SC and CO data that we need for the specified purposes. • Ensure that we have sufficient SC and CO data to properly fulfil the specified purposes. • Periodically review SC and CO data, and delete or archive anything that we don't need in line with our Data Retention Policy and Schedule.
Principle (d): accuracy
<p>The Council will:</p> <ul style="list-style-type: none"> • Maintain appropriate processes, through our relevant data protection policies, to ensure the accuracy of SC and CO data we collect. We will take particular care to do this where our use of this data has a significant impact on individuals.
Principle (e): storage limitation
<p>The Council will:</p> <ul style="list-style-type: none"> • Ensure, through our Data Retention Policy and Schedule, that SC and CO data is retained in an identifiable form for only as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. • Erase or anonymise SC and CO data in line with the relevant period set out in our Data Retention Schedule. • Identify and record in our Data Retention Schedule any SC and CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.
Principle (f): integrity and confidentiality (security)
<p>The Council will:</p> <ul style="list-style-type: none"> • Process SC and CO data in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. • Ensure that there are appropriate organisational and technical measures in place to protect SC and CO data.

4. Retention and erasure policies

The retention period and action after retention for the categories of SC and CO data noted in section 2 above are recorded in the Council's Data Retention Schedule. SC and CO data is erased or archived in line with the Council's Data Retention Policy.

5. APD review date

This APD will be kept under review and you will be made aware of any updates to it through the Council's website. This APD was last updated on 8th September 2022.