CLEVELAND POLICE

Appropriate Policy Document – Safeguarding Special Category and Sensitive Personal Data

Policy Number	384
Policy Owner	Head of Information Management and Data Protection Officer
Version	1.0
Last Review Date	October 2022
Next Review Date	October 2025
Date of approval	4th October 2022
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	☒
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

Appropriate Policy Document – Safeguarding Special Category and Sensitive Personal Data

1. Policy statement

This policy fulfils Cleveland Police's legal obligation under section 42 and Schedule 1 of the Data Protection Act 2018 to have an Appropriate Policy Document relating to the processing and safeguarding of special category personal data used for general processing, and sensitive processing used for law enforcement purposes.

2. Purpose

This policy document outlines our sensitive processing for law enforcement purposes, our processing of special category data for general purposes, and explains:

i) Our procedures for securing compliance with the law enforcement and UK GDPR 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

Additional information about our personal data processing can also be found in our Privacy notice | Cleveland Police and staff privacy notice.

3. Underpinning procedures

As part of Cleveland Police's statutory functions, we can investigate and prosecute individuals and organisations for criminal offences committed. Cleveland Police are listed as a competent authority for the purpose of Part 3 of the Data Protection Act 2018 (DPA 2018) which applies to the processing of personal data by such authorities for law enforcement purposes.

These purposes are set out at section 31 of the 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.

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 GDPR special category data. This includes:

- 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.

Cleveland Police also process information for general purposes that are covered by the UK General Data Protection regulation (GDPR), including special category data. Schedule 1 (part 4) of the DPA 2018 outlines the requirement for an APD for special category processing under the GDPR.

3.1 Description of sensitive or special category data processed

We carry out sensitive processing for law enforcement purposes in three key areas:

- Criminal investigations
- Intelligence
- Enforcement

We carry out sensitive processing of all of the categories of data defined in Part 3 section 35(8).

We process special category data for general purposes for:

- Employment matters and to fulfil our responsibilities as an employer
- Safeguarding individuals and support services provision
- Providing safer communities through partnership working

3.1.1 Consent or Schedule 8 condition for sensitive processing

We carry out sensitive processing under section 35(3) of the 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 conditions in schedule 8 of the DPA 2018.

We may rely on any of the Schedule 8 conditions for sensitive processing for law enforcement purposes.

3.1.2 Schedule 1 conditions for special category processing

We process special category personal data under potentially all Schedule 1 conditions, except for conditions 27 (anti-doping in sport), 28 (behaviours in sport) and 31 (processing by not-for-profit bodies).

3.2 Procedures for ensuring compliance with the principles

3.2.1 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 (the Data Protection Officer's role and tasks are defined in Article 39 of the UK GDPR and s71 of the Data Protection Act 2018).
- 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.

3.2.2 Principle (1): lawfulness, fairness and transparency

Processing for law enforcement must be lawful and fair. The processing must also be transparent when processing for general purposes. 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 any of the Schedule 8 conditions necessary for law enforcement processing.

Special category processing is only permissible under UK GDPR Article 9 or Article 10, providing that a Schedule 1 condition is met.

In circumstances where we seek consent, we make sure:

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

Privacy information is published on our website, we also provide privacy information at point of collection of data where applicable.

3.2.3 Principle (2): purpose limitation

We process personal data for all of the law enforcement purposes listed at section 31 of the 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.

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.

Our purposes for processing special category data are limited to ensure we fulfil our responsibilities as an employer, we safeguard individuals and support services provision. We also work towards providing safer communities through partnership working.

3.2.4 Principle (3): data minimisation

We do not systematically collect or harvest sensitive personal data for law enforcement or general 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.

Where sensitive or special category personal data is provided to us or obtained by us but is not relevant to our stated purposes, we will erase it.

3.2.5 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 erase or rectify it, we will document our decision. Some information will not be subject to amendment or update, for example where evidence has been provided at a snapshot in time.

With regards law enforcement processing, we, as far as possible, distinguish between personal data based on facts and personal data based on personal assessments or opinions and mark the file to reflect the distinction. There are circumstances where this is not possible.

Where the personal data is relevant to the purpose being pursued, we as far as possible, distinguish between personal data relating to different categories of data subject, such as:

- People suspected of committing an offence or 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 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 verifying 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.

3.2.6 Principle (5): storage limitation

We retain sensitive data for law enforcement processing in line with legislation such as Police and Criminal Evidence Act, Criminal Procedure and Investigations Act, Protection of Freedoms Act and guidance from the College of Policing, the National Police Chief's Council, the Home Office, the HMICFRS and our corporate retention schedule, unless there is a legitimate reason to retain it for longer.

All special category data processed by us is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. 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.

3.2.7 Principle (6): security

Electronic information is processed within our secure networks or with secure Cloud providers. Hard copy information is processed within our secure premises. 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.

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

3.3 Retention and erasure policies

We have a corporate retention schedule which includes personal information processed for law enforcement and general purposes.

Our retention and erasure practices are set out in our retention schedule.

3.4 APD review date

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

3.5 Assurances when sharing information

On a case by case basis, departments may wish to consider seeking assurances and policy documents equivalent to this, from third party organisation who we share sensitive and special category data with.

4. Compliance and monitoring

The Head of Information Management and Data Protection Officer is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Information Management and Data Protection Officer will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

5. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

The following identifies all version changes.

Version	Date	Reason for update	Author
1.0	Oct 2022	New policy published following approval at EMB	[redacted]