



## Leicestershire Police

### Special Category (Sensitive) Processing of Personal Data

|                         |                        |
|-------------------------|------------------------|
| Policy Owner:           | Information Manager    |
| Department Responsible: | Information Management |
| Chief Officer Approval: | DCC                    |
| Date of Next Review:    | November 2025          |

**This policy has been reviewed against APP and all relevant procedures.**

|               |                              |
|---------------|------------------------------|
| Moved to APP: | Not Moved to APP             |
| Rationale:    | APP not yet written for this |

**This document has been produced in conjunction with the Leicestershire Police Legislative Compliance Pack**

#### Review log

| Date       | Minor / Major / No change | Section                                                            | Author                                                                   |
|------------|---------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------|
| 26/10/2018 | Live                      | All                                                                | Simon Adams / Angela Middleton                                           |
| 07/10/2020 | Minor                     | 'Introduction' changed to 'Statement'. Sentence added to Statement | Angela Middleton                                                         |
| 12/10/2020 | Approval                  | All                                                                | Approved by IM Manager. Also approval for inclusion on external website. |
| 23/09/2022 | No change                 |                                                                    | Steven Morris                                                            |
| 15/11/2023 | No change                 |                                                                    | Steven Morris                                                            |
| 24/10/2024 | No Change                 |                                                                    | Steven Morris 7022                                                       |
|            |                           |                                                                    |                                                                          |
|            |                           |                                                                    |                                                                          |
|            |                           |                                                                    |                                                                          |
|            |                           |                                                                    |                                                                          |

---

## 1. Statement

Having this policy in place is a legal requirement under Part 3, Section 35 of the Data Protection Act 2018 (DPA 2018). The legislation requires the Chief Constable as Data Controller, to have an appropriate policy document (APD) in place when processing sensitive personal information for law enforcement purposes.

This policy also applies to the processing of 'special category' data defined as such under the General Data Protection Regulation 2016/679 (GDPR)

Leicestershire Police have a duty to obtain and use a wide variety of information including personal and special category information) in order to discharge its responsibilities and provide appropriate policing to the communities it serves. When it collects and uses information about individuals and/or groups it should do so in compliance with current legislation and with respect to the rights and freedoms of individual subjects within the wider community. This policy seeks to ensure that we discharge those obligations in an informed, effective and legally compliant manner.

The requirement for the APD, is to emphasise the need for greater protection when processing such information

## 2. Aims

This policy aims to:

- Ensure that processing of special category (sensitive) personal data by the Controller and his agents or by a processor on behalf of the controller is lawful.
- Ensure compliance with 'The first data protection principle' fair and lawful processing, as outlined in sections 35 of the DPA 2018 and the safeguards set out in section 42 of that Act.
- Ensure that the conditions for sensitive processing under Schedule 8 of Part 3 of the DPA 2018 are appropriately applied and met.
- Ensure appropriate granularity when recording consent if relied upon for sensitive processing of data.
- Ensure that where consent is not given, that processing is necessary for the performance of a task carried out for law enforcement purposes.
- Ensure the organisation respects the data subjects' rights and freedoms by appropriate and careful consideration and application of the exemptions and caveats laid out in sections 15, 16, 24, 25, 44 through 50 and Schedules 2, 3, 4 and 8 of the DPA 2018.

## 3. Scope

This policy applies to all police officers, police staff and all other individuals working with or on behalf of the Leicestershire police, involved in the collection, recording, processing, using, retention, review and disposal of all personal information categorised as 'Special Category personal data' under EU Regulation 2016/679 – the General Data Protection Regulations (GDPR) or as 'sensitive personal data' for the purposes of processing under the DPA 2018.

This policy must be read in conjunction with the associated policies and procedures highlighted at the end of section 5 below. This should enable the reader to apply the 6 data protection Principles outlined in the DPA 2018 and our legal obligations regarding processing, retention and erasure of sensitive information.

For the purposes of this policy and processing by consent “sensitive processing” means:—

- a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- c) the processing of data concerning health;
- d) the processing of data concerning an individual's sex life or sexual orientation.

Where data is not processed by consent but under one of the conditions set out in Schedule 8 of the DPA 2018 then sensitive processing would be for one or more of the following purposes:

- a) Statutory purposes (rule of law or substantial public interest).
- b) Administration of Justice.
- c) Protecting the Vital Interests of the data subject or another individual.
- d) Safeguarding children and other individuals at risk.
- e) Where personal data is already in the public domain.
- f) Legal Claims (proceedings, advice etc.)
- g) Courts or other judicial authorities acting in their judicial capacity.
- h) Fraud Prevention
- i) Archiving in the public interest, for scientific or historical research or statistical purposes.

In every case the reason for processing must be lawful and compliant with Part 2, section 8 of the DPA 2018 and / or Article 6 of the GDPR (Lawfulness of Processing).

The need for the processing and where appropriate the consent to process MUST be recorded in such a manner as to ensure that there is no question as to whether the consent is true or otherwise and should be a positive act such as a signed statement or audio recording where possible. If this is not the case then the full circumstances behind the necessity to process and the considered risks of not seeking consent must also be documented.

Please note that under the DPA 2018 a ‘Law Enforcement Purpose’ is defined as:-

*“ the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security”*

This is subtly different from our policing purposes as outlined in the APP and Common Law but covers the same ground.

#### **4. Legal Basis**

The implementation of the Data Protection Act 2018 (DPA) has seen the requirement for a policy document to be put in place by police forces to cover sensitive processing for Law Enforcement Purposes. This is a requirement of

sections 35(4) & (5) of the DPA when relying on the consent of the data subject or on a condition specified in Schedule 8 of the Act.

Examples of sensitive or special category personal data provided to the Force will include:

During the course of applying to join the Force as a police officer or police staff where we request:

- Racial or ethnic origin;
- Offences and alleged offences;
- Any criminal proceedings including outcomes and sentences;
- Cautions
- Personal identifier(s) e.g. tattoo.

During employment or service with the Force, it may be necessary to request provision of:

- Physical identifiers including DNA and fingerprints;
- Information relating to health and safety incidents, and accident details;
- Details to be recorded in occupational health records;
- Details for including in personal development records;
- Sound and visual images;

An individual's engagement with the Force may be as a result of falling into one or more of the following categories: i.e. as a witness, victim, relative, offender or suspect, or when passing information to the Force for law enforcement purposes.

As a result, it may be necessary to process an individual's:

- Political opinions;
- Religious or other beliefs of a similar nature;
- Details of a physical or mental health condition including medication, medical procedures etc.;
- Details of any offences and alleged offences, criminal proceedings, outcomes, sentences and cautions;
- Sex life or sexual orientation;
- Physical identifiers including DNA, fingerprints and other genetic samples;
- Photographs including footage from body worn video.

Where 'sensitive or special category' information provided consensually by an individual falling into any of the above categories or where such data has been obtained for the purposes of law enforcement; the category the provider falls into, must be clearly recorded. This will ensure the Force is able to differentiate between information collected consensually, in which case consent can be withdrawn, putting an obligation on the Chief Constable as Data Controller, to cease processing and remove the data. Equally, where the 'sensitive or special category' information is collected as a result of a Schedule 8 condition, then the condition under which the data has been obtained must be recorded. This enables the identification and removal of the data after the 'relevant period' (6 months from collection), or to ensure it is subject of review at the end of the 'relevant period' and further retention justified.

Where further retention is justified, the reason(s) must be recorded. In such cases reference may be made to the NPCC Retention and Disposal Schedule 2017.

The Force may only use the minimum amount of personal information necessary to fulfil or in connection with the particular purpose or purposes for which it has been collected, irrespective as to whether the data is recorded on a computer, in a pocket book or paper record such as a file or as an image including CCTV images.

The Force will ensure that information identified as 'sensitive' or defined as 'special category' data is handled securely, according to the requirements of Principle 6 GDPR and only accessed on a 'need to know' basis.

Other Acts considered in the drafting of this policy:

- Police Act 1996
- Human Rights Act 1998
- Freedom of Information Act 2000.
- Code of Practice (2005) for the Management of Police Information

## **5. Monitoring**

This policy will be monitored to ensure effective compliance. Monitoring will be the responsibility of the policy owner, who will be responsible for developing and reviewing this policy

Active monitoring will be undertaken by supervisors deployed into all relevant business areas.

This monitoring will:

- Ensure this policy has been put into practice
- Check that all the elements are operating properly
- Verify that any published procedures are being applied and complied with
- Ensure the aims of the policy are being achieved

Staff engaged within business areas will also be expected to undertake personal responsibility to ensure the policy is adhered to.

Monitoring is also a way of ensuring the policy does not discriminate against certain groups (this information is contained within the Equality Impact Assessment).

Compliance Auditors from within the Information Management Section will be responsible for the auditing of Force records management processes.

Other points of reference associated with this policy include:

College of Policing Information Assurance Authorised Practice

NPCC Retention and Disposal Schedule 2017

Retention Guidelines for Nominal Records on the Police National Computer

College of Policing guidance on the Management of Police Information

## **6. Review**

This policy will be reviewed on an annual basis or sooner should there be a change in legislation or subject of case law.