Appropriate Policy Document: sensitive processing for Law Enforcement Purposes, under Part 3 Data Protection Act 2018 (DPA 2018)

Version 1 September 2021

1 Introduction

This document is one of two Appropriate Policy Documents for the National Police Chiefs' Council (NPCC).

It sets out the safeguards the NPCC has in place for sensitive processing carried out for a law enforcement purpose (defined at Section 31 DPA 2018) when acting in its capacity as a competent authority. It has been produced in accordance with obligations under Sections 35(4) and 35(5) DPA 2018 and meets the requirements in Section 42 DPA 2018 (Safeguards: sensitive processing).

It should be read alongside the NPCC's Data Protection Policy and its Records of Processing Activities, (maintained in accordance with Section 61 DPA 2018).

Scope

This policy applies to sensitive processing – as defined in Section 35(8) DPA 2018 – undertaken by the NPCC in accordance with Part 3 DPA 2018.

NPCC processing of special category data for general purposes is covered in a separate Appropriate Policy Document: processing special categories and criminal convictions data under UK General Data Protection Regulation (GDPR) and Part 2 DPA 2018.

The purpose of this policy is to explain:

- NPCC procedures which are in place to secure compliance with the data protection principles set out in Part 3 DPA 2018 when sensitive processing is carried out by the NPCC (in its capacity as controller) on the basis of 'strict necessity' in reliance on one of the conditions set out in Schedule 8, or (in rare cases) on the basis of 'consent'; and

- NPCC policies about the retention and erasure of such personal data, including an indication of how long such data is to be kept.

Legal obligation

Section 35(3) DPA 2018 (the first data protection principle: law enforcement processing) provides sensitive processing (as defined in Section 35(8) DPA 2018) for any of the law enforcement purposes is permitted only in the two cases set out in sections 35(4) and (5):

- 35(4): where the data subject has given consent to the processing for the law enforcement purpose; or,
- 35(5): the processing is strictly necessary for the law enforcement purpose and it meets at least one of the conditions in Schedule 8.

An additional requirement for both conditions - arising from Section 42 (2) and (3) DPA 2018 - is that the controller must, at the time the processing is carried out, have an Appropriate Policy Document in place.

NPCC officers and staff must therefore have regard to this document when carrying out sensitive processing, when the NPCC acts in its capacity as the competent authority and controller of the personal data. When the NPCC acts in the capacity of a processor it will do so in accordance with the instructions and policies set by the controller in each case.

The NPCC has considered whether in the course of its official functions there are additional types of data that should be treated as sensitive processing although not prescribed as such under the Law Enforcement Directive and Part 3 of the Data Protection Act 2018. Consequently the NPCC may in practice voluntarily decide on a case-by-case basis to apply the enhanced safeguards to other data that it processes – this will include scenarios where it is more practical for the NPCC to treat all data as sensitive processing (even when it is not legally necessary or required to be processed as such).

2 Conditions for sensitive processing

Organisations that have a law enforcement function and are designated as competent authorities can process personal data for law enforcement purposes – defined in Section 31 DPA 2018, which includes processing for the purpose of the prevention, detection, investigation or prosecution of criminal offences – and when they do, such processing must be in accordance with Part 3 DPA 2018.

As a body established in accordance with a collaboration agreement under Section 22A of the Police Act 1996 the NPCC is a competent authority in accordance with Schedule 7, para 17, DPA 2018 in respect of the law enforcement activities it carries out as part of its official functions.

The NPCC is most likely to carry out 'sensitive processing' for a law enforcement purpose on the basis of 'strict necessity' under Section 35(5) DPA 2018. It is also able to rely on consent under Section 35(4) 2018, but this is very unlikely to be relied upon by the NPCC in the context of law enforcement processing.

The NPCC is required to have this Appropriate Policy Document in place for both scenarios, and when relying on the Section 35(5) DPA 2018 condition to permit such processing to also meet at least one of the additional conditions prescribed in Schedule 8 DPA 2018.

The Schedule 8 DPA 2018 conditions for sensitive processing that the NPCC is most likely to rely on are:

- Paragraph 1, 'Statutory etc purposes', where the sensitive processing is necessary to fulfil one of its official law enforcement functions and/or is in accordance with its responsibilities under the Common Law Policing purposes or under legislation, and where the processing is necessary for reasons of substantial public interest; for example, conducting or participating in criminal investigations;
- Paragraph 2, 'Administration of justice', for example, for processing in relation to the prosecution of offences;
- Paragraph 4, 'Safeguarding of children and of individuals', for example, where the sensitive processing is necessary to protect an individual, such as a child or a person at risk;
- Paragraph 5, 'Personal data already in the public domain', for example, if considering information available via the internet when deciding whether to proceed with an investigation;
- Paragraph 6, 'Legal claims', for example, for processing in relation to claims made against the NPCC.

The NPCC may on occasion also rely on other conditions in Schedule 8 DPA 2018, such as:

- Paragraph 3, 'Protecting individual's vital interests';
- Paragraph 8, 'Preventing fraud';
- Paragraph 9, 'Archiving etc.'

This list is not exhaustive. Further details of the NPCC's processing activities and the conditions it relies

upon are set out in its Record of Processing Activities. Details of the NPCC's functions are set out in the organisation's Privacy Notice and elsewhere on its website.

3 Compliance with data protection principles

Section 34 DPA 2018 sets out the data protection principles which apply to the processing of personal data by a competent authority for a law enforcement purpose. The procedures the NPCC has in place to ensure compliance with these when carrying out sensitive processing are set out below.

a) Accountability principle

The NPCC has put in place appropriate technical and organisational measures to meet the requirements of accountability (as required by Section 34(3) DPA 2018). These include:

- the appointment of a Data Protection Officer (DPO) who has a key assurance, compliance and advisory role on data protection matters within the NPCC;
- a direct reporting line from the DPO to our highest management level, the Chair of the NPCC, and participation at the NPCC Audit & Assurance Board;
- the development and regular review of data protection policies and guidance for officers and staff setting how the NPCC meets its data protection obligations – such as when and how a Data Protection Impact Assessment (DPIA) should be completed; and how to ensure new projects, applications or systems meet the legislative, technical and organisational requirements set out within UK data protection legislation;
- the development of more detailed local guidance relevant to the processing taking place within each business area;
- the appointment and training of Information Asset Owners (IAOs) to be responsible for the management of assigned information assets, including the identification and mitigation of risks arising from the processing of personal data, and ensuring the appropriate documentation is maintained for each of our processing activities;
- implementing appropriate security measures in relation to the personal data we process by using guidance, and processes (such as the DPIA) to ensure officers and staff access to personal data and/or to systems containing such are limited and monitored;
- regularly reviewing of our accountability measures, and updating or amending them when required, and ensuring we take a 'data protection by design and default' approach to our activities, including the design of NPCC systems.

Further information can also be found in our Data Protection Policy which sets out the ways in which the NPCC complies with data protection legislation (including integrating data protection by design and default). The NPCC may also produce subject-specific Appropriate Policy Documents as a supplement to this document if the processing of special category data requires very specific handling or in order to cater for very specific needs of the data subjects.

b) Principle 1 - 'lawfulness, fairness and transparency'

Lawful

The lawfulness of the NPCC's processing for law enforcement purposes is in most cases derived from its official functions as a policing organisation and Common Law/statutory powers, and by additionally ensuring all processing is necessary and proportionate to the identified law enforcement purpose (see 'data minimisation' below).

The NPCC's law enforcement functions include processing personal data for the prevention, detection, investigation and prosecution of crime and terrorist offences; and safeguarding against, and the prevention of, threats to public safety.

Strictly Necessary

When the NPCC carries out sensitive processing it will mainly be in reliance on the 'strictly necessary' criteria (Section 35(5) DPA 2018), and must meet at least one of the permitted conditions set out in Schedule 8 DPA 2018 – the ones the NPCC is most likely to rely on are listed in section 2 above.

Before carrying out sensitive processing NPCC officers and staff must undertake an assessment to determine whether the proposed processing is strictly necessary for and proportionate to the specified law enforcement purpose being pursued and the Schedule 8 DPA 2018 condition, and whether it will serve a substantial public interest. If the aim could be achieved by other means -- such as by not processing the data, or limiting the processing to data that is not sensitive, or by using an anonymised version – the sensitive processing will not take place.

The NPCC ensures officers and staff who might carry out sensitive processing are trained to understand their obligations when processing personal data, and provided with local guidance specific to the area of law enforcement work they are engaged in on how to assess and record their decision-making on a case-by-case basis about whether the processing is strictly necessary etc.

Consent

The NPCC is also able to rely on consent as permitted by Section 35(4) DPA 2018 as the basis for its sensitive processing. While this is unlikely to be being relied upon, were it necessary to do so we would ensure data subjects are provided with a Privacy Notice, that explicit consent for each data item was sought, that data subjects were informed they have the right to withdraw their consent at any time, they are provided with details of how they can do this, and that the NPCC has processes in place to easily facilitate any withdrawal of consent.

Further details of when the NPCC relies on specific conditions are set out in its Record of Processing Activities.

Fairness and Transparency

Detailed information about how the NPCC uses personal data, including special category data, is published in the NPCC's Data Protection Policy, Information Code of Conduct and its Privacy Notice

Further information about what the NPCC does is also published on the NPCC website.

As a policing body the NPCC is also bound by the College of Policing's Code of Ethics and complies with the College of Policing's Authorised Professional Practice on Information Management. Both are followed to ensure appropriate and responsible data use. The NPCC conducts Equality Impact Assessments (EIAs) where appropriate to assess the fairness and likely impact of policy decisions on particular groups and to ensure it develops policies and delivers services which are fair and just.

c) Principle 2 - 'specified, explicit and legitimate'

The NPCC only carries out sensitive processing when permitted to do so by law. Such personal data is collected for specific, explicit and legitimate purposes and will not be further processed for reasons that are incompatible with the purposes for which the data was collected (unless allowed for under Section 36(2) DPA 2018).

Its Privacy Notice is used to inform individuals of the legitimate purposes for which data will be processed, and the NPCC uses the measures outlined above to ensure it meets these requirements.

d) Principle 3 - 'adequate, relevant and not excessive'

The NPCC will in each case collect only the personal data that is needed for the particular law enforcement purpose/purposes of its processing, ensuring it is necessary, proportionate, adequate and relevant.

The NPCC has measures in place to ensure personal data is sufficient for the purpose(s) for which it is

used or likely to be used. The personal data must be clear in meaning and sufficient for others to understand at the present time and in the future. Those officers and staff creating or collecting personal data must ensure that it is adequate, unambiguous and professionally worded. Opinions must be distinguishable from matters of fact.

To establish relevance, a necessity test may be used to identify the minimum amount of personal data that is required to achieve the specific purpose(s). Some processing operations, such as those necessary for a major crime investigation, may require the use of a great deal of a suspect's data subject's personal data. In other circumstances only a minimal amount may be necessary. The NPCC accepts that it is excessive to hold a class of data on all individuals where that particular item of data is only relevant in certain individual cases. The NPCC adopts practices to ensure that personal data that fails to meet the requisite criteria for relevancy is either brought up to those criteria or rejected. When determining relevance consideration must be given to the necessity and proportionality of processing the personal data. Personal data must not be excessive in relation to the purpose for which it is held. It is difficult to argue that irrelevant information is not also excessive information.

NPCC internal guidance, training and policies require officers and staff to use only the minimum amount of data required to enable specific tasks to be completed. Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified/pseudonymised data sets.

e) Principle 4 - 'accurate and up to date'

The NPCC has measures in place to ensure personal data is accurate and there is a distinction as far as is possible between fact-based and opinion-based personal data.

We have measures in place to take reasonable steps to ensure inaccurate data is erased or rectified without delay having considered the purpose of the processing. We also take reasonable steps to ensure inaccurate, incomplete, or out-of-date personal data is not transmitted or made available, and if the transmission turns out to be incorrect or unlawful the recipient will be notified without delay.

Accuracy may be achieved by:

- Ensuring as far as possible that the source of the personal data is reliable, or the degree of reliability is know;
- Taking steps to verify the personal data, if possible, with another source or if reasonable, with the data subject, at the time of collection or at another convenient opportunity;
- Using automatic validation procedures to ensure procedures for data entry and the information system itself does not introduce inaccuracies;
- Using constrained fields in computer databases.

Personal data that is presented as an opinion and does not claim to be fact cannot be challenged on the grounds of inaccuracy.

We will keep personal data up-to-date 'where necessary'. The purpose for which the personal data is held or used will be relevant in deciding whether such updating is necessary. If the personal data is intended to be used merely as an 'historical' record or snapshot in time then updating would be inappropriate. Updating could involve either replacing older personal data with equivalent newer personal data or through appending the newer personal data to the older personal data. The latter approach is likely to be used where the NPCC become aware of an offender's new home address, but there remains an operational requirement to maintain records of their previous addresses.

Where relevant and as far as is possible we will ensure the personal data provides a distinction between suspects, offenders, victims (included alleged victims), and witnesses or other people with information about offences. The likelihood is that in all but exceptional cases NPCC information systems will readily and clearly identify the status of data subjects within the classifications under this part of the DPA 2018. It is also likely that some individuals will be recorded in one or more of the categories depending on the context – for example a convicted person may also the victim of crime.

f) Principle 5 - 'kept no longer than is necessary'

The NPCC manages the review, retention and disposal of personal data in accordance with its National Guidance on the Minimum Standards for the Retention and Disposal of Police Records and the College of Policing's Authorised Professional Practice on Information Management.

All personal data processed subject to sensitive processing by the NPCC is, unless retained longer for archiving purposes, retained for the periods set out in these policies. NPCC retention schedules are reviewed regularly and updated when necessary.

g) Principle 6 - 'processed in a secure manner'

Relevant NPCC IT systems are designed to ensure to the greatest extent possible personal data cannot be corrupted when it enters or is processed within them; this includes ensuring adequate security for example to guard against hackers who might try to corrupt the data, and a method for monitoring the ongoing integrity of inputted data.

The NPCC complies with security standards and policies based on industry best practice and government requirements to protect information from relevant threats. We apply these standards whether NPCC data is being processed by our own officers and staff, or by a processor on our behalf.

All officers and staff handling NPCC information or using an official system must have the appropriate security clearance and are required to complete annual training on the importance of security, and how to handle information appropriately.

In addition to having security guidance and policies embedded throughout NPCC business, the NPCC also has access to specialist security, cyber and resilience officers and staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

4 Monitoring and review

The NPCC will formally review this document not less than six months after its introduction and yearly thereafter.

This document will be made available to the Information Commissioner's Office on request.

Effective Date	1st September 2021
Last Revision Date	-
Next Revision Date	1st March 2022
Approved by	NPCC DPO
Audience	All NPCC Officers and Staff, Public