Appropriate Policy Document: processing special categories and criminal convictions data under UK General Data Protection Regulation (GDPR) and Part 2 Data Protection Act 2018 (DPA 2018)

Version 1.0 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 National Police Chiefs' Council has in place to protect special category and criminal convictions data that it processes in accordance with Article 9 UK GDPR and Article 10 UK GDPR, and has been produced in accordance with the NPCC's obligations under UK data protection legislation (Schedule 1 Part 4 DPA 2018).

It should be read alongside the NPCC's Data Protection Policy and its Record of Processing Activities, (maintained in accordance with Article 30 UK GDPR).

Scope

This policy applies to the processing of special category data – which is defined in Article 9(1) UK GDPR – processed in accordance with the UK GDPR/Part 2 DPA 2018.

The NPCC processing of special category data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by the NPCC in its capacity as a competent authority and falls under Part 3 DPA 2018 and is subject of the NPCC's other Appropriate Policy Document.

The purpose of this policy is to explain:

- NPCC procedures that are in place to secure compliance with the UK GDPR data protection principles when relying on 'substantial public interest' conditions in Part 2 of Schedule 1 DPA 2018, or for the purposes of 'employment, social security or social protection' in accordance with Part 1 of Schedule 1 DPA 2018 when processing special category data;

- NPCC retention and disposal policies concerning the processing of special categories of data on grounds of substantial public interest or for the purposes of employment, including an indication of how long such data is to be kept.

Legal obligation

Special categories of personal data

Article 9(1) UK GDPR creates a general prohibition on the processing of special categories of personal data. This prohibition is disapplied if a condition in Article 9(2) UK GDPR is met in relation to the proposed processing.

Article 9(4) UK GDPR allows the conditions in Article 9(2) UK GDPR to be subject to further requirements, in particular it is worth noting that in relation to– Article 9(2)(b) UK GDPR, '*necessary for the purposes of performing or exercising obligations or rights in connection with employment, social security or social protection'*, and Article 9(2)(g) UK GDPR, '*necessary for reasons of substantial public interest*' – these will only be met if the NPCC as a controller also has an Appropriate Policy Document in place.

NPCC officers and staff must therefore have regard to this policy when carrying out processing of special category data on behalf of the organisation, when it is acting in its capacity as controller (either alone or with other organisations).

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 any cases where it is more practical for it to treat all data as special category data (even when it is not legally necessary or required to be processed as such).

Criminal convictions and offences data

Article 10 UK GDPR requires that the processing of personal data about criminal offences and convictions or related security measures can only be carried out either where it is done under the 'control of official authority' or where the processing is authorised under domestic law provided appropriate safeguards for the rights and freedoms of the data subjects concerned are in place.

Section 10(4-5) DPA 2018 sets out the requirements for the processing of such data where it is done other than under the control of official authority (i.e. it is only permitted if it meets an additional condition set out in Part 1, 2 or 3 of Schedule 1 DPA 2018).

The NPCC's processing of criminal convictions data as a controller is carried out under the control of official authority in accordance with Article 10 UK GDPR.

2 Conditions for processing Special Category data

The lawfulness of the NPCC's processing is in most cases derived from its official functions as a policing organisation, and its corporate functions as an employer, and by ensuring that all such processing is necessary and proportionate to the identified purpose.

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

When the NPCC processes special category data it does so in accordance with the requirements of Article 9 UK GDPR and Article 10 UK GDPR and Schedule 1 DPA 2018. The majority of the NPCC's processing of special category data is for the following permitted purposes in UK GDPR Article 9:

- 9(2)(b) 'employment';
- 9(2)(g) 'substantial public interest'

The NPCC is therefore required to have this Appropriate Policy Document in place, and to meet the additional conditions prescribed in Schedule 1 DPA 2018.

The NPCC may also occasionally process some special category data in accordance with other Article 9 UK GDPR conditions, such as:

- 9(2)(a) 'consent' – as a policing organisation the NPCC will very rarely rely on consent as the basis for processing. When it does, the NPCC ensures that explicit and freely given consent for each special category data item is sought, that the data subject is informed they have the right to withdraw their consent at any time, and that processes are in place to easily facilitate the withdrawal of consent;

- 9(2)(c) 'vital interests' – the NPCC may rely on this condition under certain exceptional circumstances to protect an individual's vital interests;
- 9(2)(e) data 'made public by the data subject' – the NPCC may rely on this if, for example, it checks and further processes data in the public domain to establish consistency with information already in its possession;
- 9(2)(j) 'archiving purposes' – the NPCC relies upon this condition, for example, if it were to transfer data to The National Archives and the Office of National Statistics for archival research purposes;
- 9(2)(f) 'for the establishment, exercise or defence of legal claims' – the NPCC may rely on this if, for example, it provides personal data to assist a third party in relation to their legal claim, or is required to disclose material to a claimant, and where such processing is not strictly in support of the NPCC's own public tasks;
- 9(2)(h) for the purposes of health – the NPCC may rely on this, for example, when processing Occupational Health referrals.

These other Article 9 conditions do not require an Appropriate Policy Document to be in place.

3 Compliance with data protection principles

a) Accountability principle

The NPCC has put in place appropriate technical and organisational measures to meet the requirements of accountability [as required by Article 5(2) UK GDPR]. 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'

Lawfulness

As noted above, the lawful basis for the NPCC's processing is in most cases derived from its official functions as a policing organisation, and its corporate functions as an employer, and by ensuring all processing is fair, necessary and proportionate to the identified purpose (see 'data minimisation' below) and applicable legal basis.

When processing special category data for the employment purposes the NPCC ensures the processing is necessary and proportionate to perform its duties and meet its obligations to the data subject(s) (Part 1 paragraph 1 of Schedule 1 DPA 2018). This includes processing:

- for compliance with a legal obligation in connection with employment and personnel matters (e.g. reporting Trade Union Representative data);
- personal data concerning health in connection with the NPCC's rights and duties under employment law;
- data relating to criminal convictions in connection with recruitment, discipline or dismissal.

This list is not exhaustive - further details are recorded in the NPCC's Register of Processing Activities (RoPA) and in our Privacy Information Notices.

The specific conditions under which data may be processed for reasons of substantial public interest are set out in Part 2 paragraphs 6 to 28 of Schedule 1 DPA 2018. Most of the NPCC's processing of special category data for a substantial public interest is in support of its public tasks or functions and in accordance with the purpose set out in para 6(2)(a), Part 2, Schedule 1:

- exercise of a function conferred on a person by an enactment or rule of law.

The NPCC meets the further requirements of Part 2 Schedule 1 by ensuring it only processes such data where it is in the substantial public interest and the processing is necessary and proportionate to perform the specific lawful functions of the NPCC. We do this in various ways, including by:

- providing all officers and staff with training on how to comply with the privacy and data protection legislation - all officers and staff and contractors working for the NPCC are required to complete mandatory e-learning, which includes up-to-date information on how to comply with privacy and data protection legislation;
- providing tailored training and advice by the DPO across the NPCC, and via the means described in the above section on Accountability;
- using the DPIA process to ensure our collection and subsequent processing of data is appropriate;
- ensuring our IAOs are trained to fulfil their responsibilities; and
- taking the further steps set out in the 'data minimisation' section below.

The NPCC may, on occasion, rely on other conditions in Schedule 1, such as:

- para 8, 'Equality of opportunity or treatment' to ensure compliance with our obligations under legislation such as the Equality Act 2010 and Sex Discrimination Act 1970; or,
- para 10, 'preventing or detecting unlawful acts', if providing information to other law enforcement bodies;
- para 18, 'Safeguarding of children and of individuals at risk', for example, if any of our safeguarding teams identify an at risk individual for referral to policing organisations, social services, a GP, or other relevant professional;
- para 24, 'Providing information to elected representatives' such as Members of Parliament in response to a data subjects requests for assistance.

This list is not exhaustive. Further details of the NPCC's processing activities and the conditions it relies upon are set out in its RoPA.

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 - 'purpose limitation'

The NPCC only processes personal data when permitted to do so by law. 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 originally collected for the NPCC, unless that processing is permitted by law.

Where the NPCC obtains data on a basis that imposes specific purpose (or other) limitations, then such data will not be processed in any way that is incompatible with those further specific limitations.

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 - 'data minimisation'

The NPCC will in each case collect only the personal data that is needed for the particular purpose/purposes of its processing, ensuring it is necessary, proportionate, adequate and relevant. Each NPCC activity has in place measures to ensure it collects only the information necessary for one of its stated purposes for processing.

Each form or process will not prompt data subjects to answer questions and provide information that is not required, nor (as far as possible) will they require data subjects to provide the same information, such as date of birth or address, repeatedly: application forms will instruct data subjects to skip questions that either do not apply, or which they have already answered, and digital processes will be designed in the same way.

Additionally, 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 - 'accuracy'

Providing complete and accurate information is required when the NPCC processes personal data for its legitimate purposes. Data subjects are required to notify the NPCC of relevant changes in their personal data such as their name or address.

Details of how to do this will be provided at the point of data collection and/or via the NPCC website, and its Privacy Notice. NPCC IT systems are designed to allow for changes to personal data to be made, or for data to be erased where appropriate to do so.

If a change is reported by a data subject to one service or part of the NPCC, whenever possible this is also used to update other parts, both to improve accuracy and avoid the data subject having to report the same information multiple times.

Where permitted by law, and when it is reasonable and proportionate to do so, NPCC processes may include cross-checking information provided by a data subject with other organisations.

If the NPCC decides not to either erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision and, unless an

exemption applies, inform the data subject of this outcome.

f) Principle 5 - 'storage limitation'

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 special category data processed by the NPCC for the purpose of employment or substantial public interest 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.

Sensitive data processed on the basis of consent is also retained for the periods set out in these policies unless consent is revoked before then: details of how to revoke consent are provided when the data is collected, and details of how to contact the NPCC's DPO are published on our website.

g) Principle 6 - 'integrity and confidentiality'

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