

OFFICIAL

## Northamptonshire Police



If printed, copied or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy. Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

### Northamptonshire Police Appropriate Policy Document

#### Processing of Special Categories of Personal Data and Criminal Convictions etc. Data (Not Law Enforcement Processing)

November 2020

Reference Number	30/20	Version	V1.0
Department Responsible	Information Assurance Unit		
Author	Trina Kightley-Jones C1278		
Senior Owner	Natalee Wignall X0223		
Effective Date	September 2020	GSC Marking	Official
Type	Policy		

# Contents

Introduction .....	1
Description of Data Processed.....	1
Processing of Personal Data Relating to Criminal Convictions etc Data .....	2
The Data Protection Principles .....	2
How we will meet these principles in relation to special category and criminal conviction personal data .....	2
Principle 1. Lawful, fair and transparent .....	2
Principle 2. Specified, explicit and legitimate purposes .....	3
Principle 3. Adequate, relevant and not excessive.....	3
Principle 4. Accurate and where necessary kept up to date .....	3
Principle 5. Kept for no longer than is necessary .....	3
Principle 6. Appropriate Security .....	4
Principle 7. Accountability .....	4
Retention and Erasure Policies .....	5
Requests for erasure of special category personal data .....	5
Retention and Review of this Policy .....	5
Further Information .....	5
Document Control History .....	5

## Introduction

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.

Special Category Personal Data is defined in Article 9 GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric Data;
- Data concerning health;
- Data concerning a person's sex life; and
- Data concerning a person's sexual orientation

Article 9(1) of the GDPR prohibits the processing of special categories of personal data unless a specific condition in Article 9(2) is met. In addition, some of the Schedule 1 conditions for processing special category and criminal offence data require an APD to be in place which sets out and explains our procedures for securing compliance with the principles in Article 5 GDPR and policies regarding the retention and erasures of such personal data.

Criminal Conviction Data is defined in Article 10 GDPR and Section 11(2) of the DPA 2018 and includes personal data relating to the alleged commission of offences and proceedings for an offence committed or alleged to have been committed or the disposal of such proceedings, including sentencing.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

The Northamptonshire Police Privacy Notice sets out the legal basis for processing the personal data held under Part 2 of the DPA 2018. We also maintain an Information Asset Register and Record of Processing Activities that provide our specific lawful basis and retention periods for each information asset and processing activity within the Force. Access can be provided upon request.

Our processing of sensitive personal data for law enforcement purposes is not covered in this document but is detailed in a separate Appropriate Policy Document.

## Description of Data Processed

Northamptonshire Police process special category or criminal conviction personal data about our employees or members of the public that we engage with in the exercise of our policing functions.

It is likely that data processed by Northamptonshire Police will include all of the categories of Special Category Personal Data identified in Article 9 GDPR, including the processing of genetic or biometric data for the purposes of identifying individuals.

## OFFICIAL

### Processing of Personal Data Relating to Criminal Convictions etc Data

As an official authority processing personal data in accordance with Article 6 GDPR, Northamptonshire Police meets the requirements of GDPR Article 10 for the processing of personal data relating to criminal convictions etc data. There may be occasions where personal data regarding convictions or alleged offences will not be processed for our law enforcement purposes. (For example, for recruitment and vetting purposes where an employee may have existing convictions or offences not dealt with by Northamptonshire Police).

### The Data Protection Principles

The principles set out in the GDPR require personal data to be:

1. Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
2. Collected for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation);
3. Adequate, relevant and not excessive in relation to the purposes for which they are processed (data minimization);
4. Accurate and where necessary kept up to date (accuracy);
5. Kept in a form which permits identification for no longer than is necessary for the purposes for which the data are processed (storage limitation);
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational measures (integrity and confidentiality);
7. There is also seventh principle defined in Article 5(2) that provides: The Controller is responsible for and must be able to demonstrate compliance with the above.

### How we will meet these principles in relation to special category and criminal conviction personal data

#### Principle 1. Lawful, fair and transparent

Northamptonshire Police will communicate fair and transparent processing information to individuals using a range of methods, including provision of privacy notices and verbally, which will be provided at the time the information is provided to us by the data subject.

The privacy notice is also available on the Northamptonshire Police website, available by contacting the Data Protection Officer on request and in other formats if required. These notices detail the legal basis for processing types of personal data.

Where explicit consent is requested or given from an individual to allow processing of personal data this will be an affirmative action. The individual will be provided with details of what personal data are involved, what they are consenting to (e.g. the sharing of their data), what will happen to their data and the length of time the data will be retained. They will also be advised of their right to withdraw consent at any time.

Where consent is requested or given, this information and the response from the individual will be documented and available for an audit trail.

## Principle 2. Specified, explicit and legitimate purposes

Processing of personal data will be restricted to only that which is necessary for the relevant purpose and it will not be used for a matter which is incompatible with that purpose. Northamptonshire Police privacy notice details the purposes for which personal data is processed.

If we do use data for a new, compatible purpose – or where we have a clear basis in law – we will inform the data subject first and seek consent if appropriate.

## Principle 3. Adequate, relevant and not excessive

Any personal data collected for general processing purposes will be restricted to that which is necessary for the purposes of processing. The data protection training required by all officers and staff emphasises that police records must ensure that personal data is adequate, relevant, unambiguous and professionally worded. Matters of opinion, which are not fact, will be clearly recorded as such.

## Principle 4. Accurate and where necessary kept up to date

We will ensure as far as possible that the personal data we process is accurate and kept up to date. In some circumstances we may need to retain factually inaccurate information e.g. information provided by a third party which does not represent the true facts.

All officers and staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process. Checks are carried out on the accuracy of data during audits and scheduled reviews.

Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible, there will be an addendum to that personal data advising of the inaccuracy. When relevant, the processing will be restricted in accordance with Article 18 of the GDPR.

Recipients of the relevant data will be notified of the erasure, rectification or restriction in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort.

## Principle 5. Kept for no longer than is necessary

Northamptonshire Police has a Records Management Review, Retention and Disposal Policy which outlines the principles which Northamptonshire Police adhere to for the retention, review and disposal of records which have been created within its activities and functions. This policy is available on the Force website (**pending**) or available on request to the Data Protection Officer.

When an individual withdraws consent to the processing of personal data (where consent has been previously provided by the individual), that data will be destroyed on receipt of the withdrawal unless there is an overriding purpose for continued processing.

## Principle 6. Appropriate Security

Northamptonshire Police has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of all personal data processed.

**Technical measures** – Northamptonshire Police applies the information security standards set for National Policing Community by the Cabinet Office and the Home Office. This includes encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password-controlled access, technical assurance and technical audits.

**Organisational measures** – All officers and staff are required to undertake mandatory data protection training. All new staff, officers and contractors are vetted prior to being given access to Northamptonshire Police information, systems and records.

Officers and staff receive training in how to use police systems before being granted access. Buildings are kept physically secure with access only being granted to individuals who are authorised to access.

Further measures include the following Policies:

- Data Protection Policy.
- Information Security Policy and Enabling Guidance

## Principle 7. Accountability

Northamptonshire Police has in place technical and organisational safeguards to meet the requirement of accountability.

We have appointed a Data Protection Officer who reports directly to our Chief Officer Group. We have a dedicated information assurance team and a 'data protection by design and default' approach built into our processing, project management and procurement procedures. This ensures that we carry out Data Protection Impact Assessments and other risk and security assessments as applicable in relation to any potential high risk processing, have written contracts in place with any processors used and implement appropriate security measures.

We maintain appropriate documentation of our processing activities, including:

- Record of processing activities maintained by each business area.
- Information detailed in appropriate relevant privacy notices.
- Purposes of processing, lawful basis, etc. documented for specific processing activities including Data Protection Impact Assessments and Information Sharing Agreements.
- A suite of policies relating to Information Management (e.g. Data Protection, Information Security, Records Management etc.)

## Retention and Erasure Policies

Northamptonshire Police has adopted the retention rules outlined in the Authorised Professional Practice on the Management of Police Information (MoPI) and has in place record retention schedules which show how long records are retained. We have records management policies which cover the principles of review, retention and disposal.

### Requests for erasure of special category personal data

Requests for erasure of personal data will be dealt with in accordance with Article 17 of the GDPR and when relevant, recipients of the relevant data will be notified of the erasure, in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort. Any such decision will be recorded.

## Retention and Review of this Policy

This policy document will be retained in accordance with Part 4 of Schedule 1 of the DPA 2018. It will be made available to the ICO on request.

The policy will be reviewed on an annual basis (or more regularly if circumstances require it) and updated as necessary at these reviews.

## Further Information

For further information about our compliance with data protection legislation or if you wish to contact our Data Protection Officer, please contact us using the details below:

**Northamptonshire Police Data Protection Officer:** Trina Kightley-Jones

Data Protection Officer  
Northamptonshire Police Headquarters  
Wootton Hall  
Wootton Hall Park  
Northampton  
NN4 0JQ

Telephone: 03000 111 222

Email: [dataprotection@northants.pnn.police.uk](mailto:dataprotection@northants.pnn.police.uk)

## Document Control History

DATE	VERSION	INDIVIDUAL	CHANGES MADE
19/11/20	1.0 (Draft)	Christian Kirkpatrick	First draft complete.
27/11/20	1.0 (Final)	Christian Kirkpatrick	Minor adjustments, watermark removed for publishing.