Code of Practice

On the Operation and Use of the Police National Database

(Made by the Secretary of State for the Home Department in March 2010)

Code of Practice

On the Operation and Use of the Police National Database

(Made by the Secretary of State for the Home Department in March 2010)

Presented to Parliament pursuant to Section 39A of the Police Act 1996

Code of Practice on the Operation and Use of the Police National Database

CONTENTS

1. Introduction 2
2. The Purpose of the Police National Database 5
3. General Principles 6
4. Using the PND 8

1 INTRODUCTION

1.1 General

The Police National Database (PND) is a national information management system that improves the ability of the Police Service to manage and share intelligence and other operational information, to prevent and detect crime and make communities safer. The PND offers a capability for the Police Service to share, access and search local information electronically, overcoming artificial geographical and jurisdictional boundaries.

As a national system, it is crucial that both the PND and the information obtained from it are used consistently across the Police Service and in compliance with legal and policy requirements. This will provide chief officers with confidence that the information they provide to the PND is being used appropriately by other forces. The PND is one of a number of force, regional and national systems available to the Police Service. Before making use of the PND, consideration should be given as to whether it is the most appropriate system to use.

1.2 Purpose of the code

The purpose of this code and associated guidance is:

a) to promote the lawful and consistent use of the PND and the information obtained from it;

b) to ensure that chief officers adopt practices for the use of the PND and the information obtained from it in order that such information is used effectively for policing purposes;

c) to ensure that the operation of the PND complies with data protection and human rights legislation; and

d) to ensure that the PND is not used in a way which is discriminatory or otherwise unfair to anyone based on their age, race, ethnicity, any faith or belief, gender, gender identity, sexual orientation or any disability;

1.2.1 This code sets out the principles governing the use of the PND and any information obtained from it (including personal data). It covers:

a) the purpose and strategic priorities of the PND;

b) general principles applying to the operation of the PND, including accountability, security, vetting and training of users;

c) that the use of information is fair, necessary and proportionate;

d) that information is accurate and up to date;

e) that information obtained from the system is managed appropriately;

f) disclosure of the information; and

g) using the PND – including access to information, and administering and auditing the use of the PND.

Over time, the PND will develop and so the procedures for giving effect to the principles set out in this code may change. This code will, therefore, be supported by more detailed and extensive guidance that will define the standards required within forces. That guidance may change from time to time, but must be framed in compliance with the principles established by this code.

1.3 Statutory basis of the code

This code of practice comes into effect on 31 March 2010.

The code is issued by the Secretary of State for the Home Department in relation to the discharge of the functions of chief officers of police. A chief officer of police shall have regard to this code, as will the members of the police force for whom the chief officer of police is responsible.

Nothing in this code alters the existing legal powers or responsibilities of any police authority, chief officer of police, or other person.

This code of practice is made under section 39A of Police Act 1996, which permits the Secretary of State to issue codes of practice relating to the discharge of their functions by chief officers where it is necessary to do so for the purpose of promoting the efficiency and effectiveness of police forces in England and Wales.

This code recognises that there is an existing legal framework for the use of information in legislation relating to data protection and human rights.

It applies directly to the police forces maintained for the police areas of England and Wales defined in section 1 of the Police Act 1996. Under section 48 of the Railways and Transport Safety Act 2003, this code of practice also applies to the Chief Constable of the British Transport Police.

It is available for adoption by other agencies, including other police forces not covered by section 1 of the 1996 Act and law enforcement agencies within the United Kingdom that exchange information with the Police Service in England and Wales.

Chief officers must introduce arrangements within their forces for the operation and use of the PND that comply with the principles set out in the following paragraphs, and with guidance issued under this code.

1.4 Data Protection and Management of Information

Chief officers are responsible for the development and implementation of appropriate procedures and systems so that personal data is processed in accordance with the provisions of the Data Protection Act 1998 and other relevant legislation. Information which is placed on the PND must be managed in compliance with the guidance issued under the code of practice on the Management of Police Information and the Association of Chief Police Officers (ACPO) Data Protection Manual of Guidance.

Each chief officer is a data controller, in common with all other chief officers, for the personal information held on the system. As such, all chief officers share the responsibilities of data controllers set out in the Data Protection Act 1998. Where the processing of personal data is carried out on behalf of the data controllers by a data processor, such processing will only be carried out under the terms of a Data

Processing Agreement. The Agreement will be entered into by ACPO on behalf of the data controllers.

1.5 Definitions

In this code:

a) chief officer of police means:

i) in relation to a police force maintained under section 2 of the Police Act 1996, the Chief Constable,

ii) in relation to the Metropolitan police force, the Commissioner of Police of the Metropolis,

iii) in relation to the City of London police force, the Commissioner of Police for the City of London,

iv) in relation to the British Transport Police, the Chief Constable, and

v) in the case of other organisations adopting this code, their equivalents;

b) references to information include data. All information, including intelligence and personal data obtained and recorded for policing purposes and placed on the PND, is referred to as PND information;

c) unless otherwise stated, "use of the PND" includes loading information onto the system, using the system, and using the information obtained from the system;

d) a "PND User" is an individual who is registered as a PND user, has a validated user ID, can log on to the PND and directly use the PND functionality; and

e) a "PND Administrator" is an individual delegated by the chief officer of police to supervise and manage responsibility for the force's PND operations and system administration.

1.6 Role of HM Inspectors of Constabulary

HM Inspectors of Constabulary will monitor chief officers' compliance with this code, associated guidance, and standards.

1.7 Role of the National Policing Improvement Agency

The National Policing Improvement Agency (NPIA), or any successor body designated by the Secretary of State, has responsibility on behalf of the police forces of England and Wales for the development of guidance under this code. Such guidance and any subsequent amendments will be prepared in consultation with the Association of Chief Police Officers, the Association of Police Authorities, and such other persons as the NPIA thinks fit.

1.8 Guidance under this code of practice

Guidance under this code of practice will:

a) include Standard Operating Procedures, a Code of Connection, Business and System Rules; and

b) act as reference tools for users and trainers.

Guidance documents and user guides will be produced by the NPIA.

For the purpose of achieving, throughout the Police Service, the standards described above, guidance issued under this code, unless superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996, may specify procedures to be adopted within police forces for the use of the PND.

1.9 Consultation

Consultation has been carried out by the NPIA in accordance with the statutory provisions.

2 THE PURPOSE OF THE POLICE NATIONAL DATABASE

2.1 Policing purposes

The PND is to be used solely for policing purposes. For the purposes of this code, policing purposes are:

a) protecting life and property;

b) preserving order;

c) preventing the commission of offences;

d) bringing offenders to justice; and

e) any duty or responsibility of the police arising from common or statute law.

2.2 Strategic priorities

The PND enables chief officers to make more informed decisions and better risk assessments, supporting the following areas of policing:

a) Protecting children and vulnerable people, by being better able to understand the risk they are facing, and by more thorough vetting of people in positions of responsibility and trust.

b) Understanding the threat posed by terrorism of whatever nature, and helping to reduce the risk of terrorist activity.

c) Disrupting and preventing major, serious and organised crime, helping to reduce the harm caused by the most dangerous offenders.

Chief officers should prioritise the use of the PND accordingly but are free to use the PND for other policing purposes.

3 GENERAL PRINCIPLES

3.1 Lawfulness

Any use of the PND must be compliant with legal obligations, including those under:

a) the Data Protection Act 1998;

b) the Human Rights Act 1998; and

c) the common law duty of confidence.

3.2 Accountability and responsibility

Whilst this code of practice and accompanying guidance will provide advice, ultimately it is the responsibility of chief officers to decide what information to place on the system, what information to withhold from the system, and what restrictions to apply on access to and use of the information, and to accept the risks of any such decisions. Similarly, chief officers are responsible for how information on the PND is used by their force.

3.3 Intelligence

The PND is an intelligence data-handling system rather than an evidential system; it is a repository for copies of records which are held locally by forces: should PND information be required for evidential purposes it will be necessary to obtain the original information from the data provider.

3.4 Openness and transparency

Chief officers should be as open and transparent as possible about the information held on the PND and how it is used. It should be made clear that information gathered by forces may be placed on a national system and shared with other forces and other law enforcement bodies.

3.5 A policy for the use of the PND to be applied within each police force

Chief officers will establish and maintain within their forces a policy for the use of the PND, under the direction of an officer of ACPO rank or equivalent, complying with guidance and standards issued under this code unless that guidance is superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996.

3.6 Extracting and Anonymising Information

Where information is exported from the PND to conduct analysis and it is not necessary to be able to identify individuals from the information, the exported information should be anonymised by the removal of information from those fields that are capable of identifying individuals.

Data must only be extracted from the PND when necessary and lawful, and with the appropriate authorisations as set out in the associated guidance to this code.

3.7 Security of, and access to, PND information

The PND has been assessed as a CONFIDENTIAL system handling information marked up to and including CONFIDENTIAL according to the Government Protective Marking Scheme. The President of ACPO will appoint a body to authorise connections to the PND. Before a connection to the PND can be authorised, evidence of accreditation must be provided to the National Accreditor. Accreditation requires that a Risk Management and Accreditation Document Set (RMADS) must be prepared to HMG Information Assurance Standard 2 (IAS2), including a detailed technical risk assessment using HMG Information Assurance Standard 1 (IAS1). Anyone handling information gained from the PND is responsible for the storage of the information according to the protective marking or other handling restrictions applied to it.

Nothing in this code prevents non-police organisations that contribute to public protection being granted direct access to the PND in future, provided all the relevant legal, security and other requirements are met and a satisfactory case is made to the body appointed to authorise such access.

3.8 Training for staff

Guidance issued under this code will specify the training required by staff using the PND, whether as users, system administrators, auditors or in any other role. It may also identify training required by those who do not directly access the system but who may request that others use the system on their behalf, and those who may be provided with information obtained from the PND. Access to or use of the PND is restricted to those persons who have successfully completed specified training.

Training for these purposes is not only to ensure compliance with the legal framework for information management and the maintenance of high standards of competence, but also to establish the consistency of procedures throughout the Police Service.

3.9 Vetting

All users of the PND must be vetted to the appropriate level to access the information available from the PND. The vetting standards for the Police Service are determined by ACPO Vetting Policy. The vetting standards for non-police organisations will be determined by the body appointed to authorise access to the PND.

3.10 Role-Based Access Control

Role-Based Access Control (RBAC) is mandatory on the PND to ensure that users only have access to capabilities and information that they need for their business role. Users have the ability to conduct enquiries on behalf of other people; such enquiries must only be conducted for a proper purpose by an authorised PND user using their own access details.

3.11 Relationships between records

The PND will allow users to conduct complex searches which may suggest relationships between records. The determination and handling of such relationships must be lawful and in accordance with the guidance issued under this code.

3.12 Versioning and deletion of information from the PND

When updating information that is on the PND, chief officers need to ensure that a decision is made as to whether previous versions of that information should be retained with version control applied or removed.

When a chief officer decides to dispose of information from a local system, that information must also be removed from the PND.

4 Using the PND

4.1 Access to information

PND users are allocated to one or more user roles, which means that RBAC will be applied to determine which functions they can perform and which data they can access.

4.2 System administration

Chief officers should ensure that effective system administration is in place to manage user accounts, system updates and other similar functions.

4.3 Auditing

There is a need to record and retain audit log data to, amongst other things, prove the integrity of the transactional data should the need arise to do so; and to carry out a programme of monitoring to guard against the improper use of the PND.
Audit logs will record sufficient information about each transaction to enable identification of individuals (both PND users and the subjects of PND records), making the audit logs subject to the Data Protection Act and other regulatory and legislative controls.

Chief officers will normally be responsible for auditing the activity of their own personnel; however, no user should audit their own activity. The PND will provide for auditing by other forces or at a national level where this is necessary. Procedures should be put in place to ensure that adequate auditing is carried out and that appropriate action is taken where misuse is discovered.

4.4 Sharing information obtained from the PND

Information obtained from the PND may be shared, provided the sharing is lawful and conducted in accordance with the code of practice on the Management of Police Information.