Use of the Police National Computer by non-police organisations

An inspection of Thurrock Council

May 2016
© HMIC 2016
ISBN: 978-1-78655-094-1
www.justiceinspectorates.gov.uk/hmic
## Contents

**Introduction** ........................................................................................................................................... 3  
  Background and context ......................................................................................................................... 3  
  Terms of reference ................................................................................................................................. 4  
  About Thurrock Council ....................................................................................................................... 4  
  Methodology .......................................................................................................................................... 5

**Findings** ............................................................................................................................................... 6  
  Scale of PNC use ................................................................................................................................... 6  
  The level of access and authorised purposes for PNC use .................................................................. 6  
  Does the organisation comply with its Security Operating Procedures? ....................................... 7

**Conclusions** ......................................................................................................................................... 10  
  Level of access .................................................................................................................................... 10  
  Compliance .......................................................................................................................................... 10  
  Efficiency and effectiveness .................................................................................................................. 10
Introduction

Background and context

The Police National Computer (PNC) is a national database of information available to all police forces throughout the United Kingdom. In addition, certain other organisations, referred to as “non-police organisations”, have access to information held on the PNC in order to help them fulfil their statutory functions.

In such instances, access is granted by a body called the Police Information Access Panel (“the Panel”). In order to obtain access, each organisation must submit a detailed business case that satisfies the Panel that a valid and lawful requirement for access exists.

If this is the case, two documents are produced that specify the level of access permitted and the manner in which the non-police body may use the PNC: the Supply Agreement, which describes the permitted access and how it will be provided; and the Security Operating Procedures, which are a requirement of the Supply Agreement but which are produced by the non-police organisation for the attention of its staff.

Some non-police organisations access the PNC through discrete computer terminals installed in their premises. This is known as “direct access”. Other non-police organisations obtain PNC information through a third party, usually a police force. This is known as “indirect access”.

In either arrangement, the public needs to have confidence that access is properly regulated and that effective auditing arrangements are in place. This is important because much of the information held on the PNC is sensitive and personal.

Her Majesty’s Inspectorate of Constabulary (HMIC) is recognised as having strong expertise in this area and the Government’s Independent Advisor on Criminality Information Management recommended that HMIC’s audit role is extended to cover all PNC users.

---


2 The Police Information Access Panel is a sub-group of the PNC governing body – the Police PNC Policy and Prioritisation Group (known within policing as “P4G”). The Panel is chaired by a chief officer and comprises a cross-section of senior Home Office and police leaders who are concerned with the management of the PNC. The Panel meets on a quarterly basis to consider applications for access to the PNC. Her Majesty's Inspectorate of Constabulary is represented on the Panel.

Consequently, as part of our regular programme of inspections, we examine: the circumstances under which non-police organisations are granted access to the PNC; the ways in which they use PNC information; the safeguards that are required in order to protect the information; and whether those safeguards are being properly applied.

Non-police organisations are also subject to a separate Home Office audit, which examines in detail whether PNC data is held and used in an approved and secure way.

While HMIC’s inspections can be prioritised on the basis of the findings of these Home Office audits, HMIC’s inspections do not examine all of the same issues. However, there can be certain areas of overlap. Where our inspections reveal concerns in areas that are also subject to Home Office audit, we highlight this.

**Terms of reference**

HMIC’s inspections of non-police organisations that have access to the PNC aim to answer three questions:

1. Is the level of access specified in the *Supply Agreement* appropriate for the needs of the non-police organisation?

2. Does the non-police organisation comply with the *Security Operating Procedures*? In particular, are the arrangements for training, physical security, and internal audit compliant with the *Security Operating Procedures*?

3. Is the non-police organisation making efficient and effective use of the PNC?

**About Thurrock Council**

The Unitary Authority Council of Thurrock, which we sometimes refer to in this report as “Thurrock Council” and “the organisation”, has direct access to the PNC.

Access is confined to its Counter Fraud and Investigation Directorate which has 32 personnel.

---


5 The Home Office National Police Information Risk Management Team conducts audits to assure the Police Information Access Panel that PNC data is being held and used in an approved and secure manner in accordance with the supply agreement and relevant legislation including, but not limited to: the Data Protection Act 1998; the Computer Misuse Act 1990; and the Official Secrets Act 1989.
Working closely with the police, the Department of Work and Pensions (in relation to benefit fraud) and the Ministry of Justice (in relation to legal aid fraud), the Counter Fraud and Investigation Directorate is responsible for investigating financial crimes against Thurrock Council and confiscating criminal assets. Two other councils (Southend-on-Sea, in Essex and Medway, in Kent) also rely on the Thurrock Counter Fraud and Investigation Directorate for a similar purpose.

**Methodology**

This inspection took place in January 2015. Before the fieldwork stage, we reviewed documents (including the *Supply Agreement* and the *Security Operating Procedures*) in order to assist us in preparing questions for the interviews.

We invited Thurrock Council to provide us with documentary evidence of its adherence to the *Supply Agreement* and *Security Operating Procedures*. This was followed by visits to their headquarters in Grays, Essex (at which the organisation's single PNC terminal is housed). Over two days, we assessed the physical security arrangements and interviewed the staff that used the PNC. We asked the interviewees to show us how they used the PNC.

We examined Thurrock Council's internal audit process for the PNC. We looked at audit records and, through our interviews, tested interviewees' understanding of the internal audit processes and escalation procedures.

We also reviewed data, provided to us by the Home Office, on the organisation's use of the PNC.

---


7 In this context, escalation procedures are the procedures that personnel are expected to adopt when an internal audit reveals that a PNC check has been conducted for an inappropriate purpose. Generally, the procedure involves referring the matter to a manager.
Findings

Scale of PNC use

The Home Office provided us with statistics on the number of PNC checks carried out by Thurrock Council for the period 1 April 2014 to 31 December 2014. We found that 137 PNC checks in relation to people were carried out by Thurrock Council over that period. There were also 45 vehicle checks.

The level of access and authorised purposes for PNC use

We found that the level of access in the Supply Agreement was appropriate for Thurrock Council’s needs and that the organisation was using the PNC in accordance with the Supply Agreement.

Level of access

We were provided with a copy of the Supply Agreement, which was agreed between Thurrock Council and the Home Office on 28 February 2013 and was to continue in force for three years. Therefore it was current at the time of our inspection (December 2015).

The Supply Agreement specified that Thurrock Council was authorised to conduct five different kinds of PNC check:

1. Name (restricted): this type of check allowed an operator to type in the name of a person in order to determine whether the PNC holds a record of someone with that name. If such a record existed, Thurrock Council’s level of access allowed it to view certain information from that record, such as criminal convictions, arrest details and cautions. For this kind of check, Thurrock Council’s access was restricted to particular parts of the record.

2. Vehicle registration mark (basic): this type of check allowed an operator to type in a complete vehicle registration mark in order to determine if the vehicle was stolen or of interest to the police for some other reason. This type of check also revealed the name and address of the vehicle’s registered keeper.

3. Vehicle identification number: this type of check allowed an operator to type in a vehicle identification number in order to determine if the vehicle was stolen or of interest to the police for some other reason. If the name of the vehicle manufacturer was also typed in, further details including the name and address of the registered keeper would be revealed.

8 Supply Agreement LA104 Version 1.0, National Policing Improvement Agency and Thurrock Council, February 2013, Part 2 Schedule 1, paragraphs 1 and 2.
4. Postcode: this type of check allowed an operator to type in a postcode (or a combination of postcodes up to a maximum of six) in order to identify vehicles registered to an address within the area covered by the postcode that was used to make the search.

5. Transaction log: this type of check allowed an operator to type in a code in order to generate a list of previous checks carried out on the PNC. Generally this list was used for audit purposes.

**Authorised purposes**

The *Supply Agreement* stated that Thurrock Council was authorised to conduct checks in order to:

- "...allow the Fraud Investigation Department of the Council to exercise its statutory duties to investigate allegations of fraud committed against the public purse, apprehending and prosecuting offenders where appropriate".  

For the purposes of our inspection we considered the reference in the *Supply Agreement* to the "Fraud Investigation Department" to be a reference to Thurrock Council's Counter Fraud and Investigation Directorate which we described earlier in this report. Furthermore, we considered that investigations carried out by the Thurrock Council Counter Fraud and Investigation Directorate on behalf of other councils were carried out in observance of the statutory duties of those councils.

The level of access included some of the PNC's more powerful search functions, which tend to be used by the police and law enforcement agencies for detailed intelligence development purposes and in certain criminal investigations (usually where serious crimes are involved). Given the nature of the investigations carried out by the Counter Fraud and Investigation Directorate, this level of access was appropriate.

**Does the organisation comply with its Security Operating Procedures?**

We found that Thurrock Council was compliant with the requirements set out in its *Security Operating Procedures*.

**Training**

One of the requirements in the *Security Operating Procedures* is that all PNC users must receive accredited training. During the inspection we examined the relevant

---


training records. These satisfied us that Thurrock Council's two PNC users had both received accredited training from trainers employed by Kent Police.\(^\text{11}\)

**Physical security**

A further requirement of the *Security Operating Procedures* is that the PNC terminal must be located in a secure building.\(^\text{12}\)

We found that the Thurrock Council's PNC terminal was kept in a secure building. The PNC terminal was located in the offices of the Counter Fraud Investigations Directorate, within which both the PNC operators worked. Access to the building was by a locked door with a pass-code which was changed every 28 days. Access through internal doors was by swipe-card. Visitors to the building were required to be accompanied at all times.

**Internal audit**

The *Security Operating Procedures* and other related documents set out various requirements which are the subject of internal audit. These include:

- PNC personnel are required to sign a document to confirm they have read the *Security Operating Procedures* and undertake to comply with them;\(^\text{13}\)
- PNC checks may only be conducted once authorised by an 'approver' (in urgent cases, orally, otherwise in writing); and
- the frequency of audits will depend on the amount of transactions, but will ordinarily be monthly.

In relation to the first requirement, we examined the documentation and were satisfied that both PNC personnel had signed the appropriate document.

In relation to the second requirement, we found that requests for PNC checks were made by completion of an application form that was forwarded to the head of investigations for approval. If declined, the form was retained by the head of investigations; if approved, the form was forwarded to a PNC operator for the check to be carried out. The result was printed and posted to the enquirer.\(^\text{14}\)

The audit records we examined indicated that, for both urgent and non-urgent cases, the requirement for approval of each PNC check was being met.

---

11 The College of Policing is responsible for the accreditation of PNC training providers.


13 *Ibid.* Appendix B.

We did not find any instances where PNC checks had been conducted without approval.

In relation to the third requirement, we found that Thurrock Council was auditing all of its PNC checks monthly. Because of the low numbers of checks, the 100 percent audit was not an onerous task for the organisation.

We also found clearly defined procedures for the escalation of issues of concern to managers. Although we did not find any instances where concerns had been escalated, those we interviewed were aware of and understood the procedures.
Conclusions

Level of access
Taking into account the purposes for which Thurrock Council needs PNC access, we conclude that the level of access specified in the Supply Agreement is appropriate for the Council's needs.

Compliance
The satisfactory training records, the physical security arrangements, the signed undertakings by all PNC staff and the high level of internal audit lead us to conclude that the Council has been complying with the requirements of its Security Operating Procedures.

Efficiency and effectiveness
We conclude that Thurrock Council is making efficient and effective use of the PNC.