Use of the Police National Computer by non-police organisations

An inspection of the Children and Family Court Advisory and Support Service

May 2016

ISBN: 978-1-78655-093-4

www.justiceinspectorates.gov.uk/hmic

Contents

Introduction

Background and context

The Police National Computer (PNC) is a national database of information available to all police forces throughout the United Kingdom.[1] 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").[2] 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.[3]

---

[1] *Police National Computer (PNC) Guidance: version 5*, Home Office, January 2014, page 5. The PNC holds information concerning people and property, including convictions, wanted and missing people, stolen vehicles and other types of stolen property.

[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.

[3] *A Common Sense Approach: a review of the criminal records regime in England and Wales*, Sunita Mason (Independent Advisor for Criminality Information Management), November 2011, pages 34-35.

Consequently, as part of our regular programme of inspections,[4] 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.[5]

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 the Children and Family Court Advisory and Support Service

The Children and Family Court Advisory and Support Service, which we refer to in this report as "Cafcass"[6] or "the organisation", has direct access to the PNC.

[4] *HMIC's 2015/16 Inspection Programme: An inspection framework prepared under Schedule 4A to the Police Act 1996*, HMIC, March 2015, page 11. Available from: www.justiceinspectorates.gov.uk/hmic/publications/hmic-inspection-programme-2015-16/

[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.

[6] Although Cafcass is an acronym for the Children and Family Court Advisory and Support Service, the organisation uses Cafcass as its name – see www.cafcass.gov.uk

Cafcass was formed in 2001 and is accountable to Parliament through the Ministry of Justice. The organisation's principal objective is to look after the interests of children involved in family proceedings in England. Cafcass is independent of the courts and social services, but operates under the rules of the Family Court to work with children and their families and advise the courts on what it considers to be in the best interests of individual children.[7]

When involved in such cases, Cafcass conducts a range of enquiries into the people concerned. This is done in order to safeguard children.[8] These enquiries include checks of the PNC.

Methodology

This inspection took place in March 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 Cafcass to provide us with documentary evidence of its adherence to the *Supply Agreement* and *Security Operating Procedures*. This was followed by a visit to the Cafcass offices in Coventry where their PNC unit is based. This unit obtains PNC data for case workers based at the 45 Cafcass sites across England. Over two days, we assessed the physical security arrangements and interviewed a cross-section of staff who used the PNC, including the manager, supervisors and PNC operators. We asked interviewees to show us how they used the PNC.

We examined the organisation'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.[9]

We also reviewed data relating to Cafcass' use of the PNC. These data were provided to us by the Home Office.

[7] See www.gov.uk/government/organisations/children-and-family-court-advisory-and-support-service.

[8] *Cafcass Operating Framework*, downloaded 14 March 2016 from www.cafcass.gov.uk/media/212819/cafcass_operating_framework.pdf.

[9] 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 Cafcass for the period 1 November 2014 to 28 February 2015. We found that 42,568 PNC checks in relation to people were carried out by Cafcass over that period. There were also 19 transactions that enabled the manager to check that use of the PNC had been legitimate.

The level of access and authorised purposes for PNC use

We found that Cafcass had access to and was making use of the PNC even though the *Supply Agreement* had expired.

Notwithstanding the lack of a current *Supply Agreement*, we found that the level of access available to Cafcass was sufficient to enable basic checks on people. We also found that this level of access was sufficient to meet the needs of Cafcass.

Level of access

We were provided with a copy of the *Supply Agreement*, which was agreed between Cafcass and the National Policing Improvement Agency on 31 October 2011 and was to continue in force for three years. It therefore ceased to be valid on 31 October 2014. We found that Cafcass continued to have access to and make use of the PNC after that date and at the time of our inspection in 2015.

The *Supply Agreement* specified that Cafcass was authorised to conduct two 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, the Cafcass 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, access was restricted to particular parts of the record.

2. 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. [10]

[10] *Supply Agreement Version 1.0,* National Policing Improvement Agency and Cafcass, October 2011, Part 2 Schedule 1, section 1.

Authorised purposes

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

"Identify any safeguarding risks relating to parties and children named on the application submitted to Cafcass and to enable to identify and report to the Court with regards to:

- sexual/physical abuse and/or neglect
- domestic violence
- other violence
- drugs and/or alcohol abuse
- threats of abduction
- emotional harm
- inter-parental conflict – e.g. the nature of the court proceedings
- adults who represent a risk to children
- any other specific cause for concern for the welfare of the child, including all categories of risk to children".[11]

During our interviews with the manager and staff, we found that when Cafcass carried out a PNC check it sometimes discovered that the person checked was wanted by the police. In such cases Cafcass did not always notify the police force concerned that a person wanted by them had come to the organisation's attention. Instead, decisions were made about whether to notify the police on a case-by-case basis. The manager informed us that the organisation has a statutory responsibility to children and always notifying the police in such cases could affect adversely the welfare of a child.

We brought to the attention of Cafcass managers that this practice contravened the (expired) *Supply Agreement*, which stated: [12]

> "Should the Customer, in the course of their work on the PNC, discover information that would be of importance to the police (for example, a notification of wanted or missing on the record of the person being checked), they will undertake to notify the police force that requires the information, their

[11] *Ibid.,* Part 2 Schedule 1, section 2.

[12] *Ibid*., Part *2* Schedule 1, section 4.

local police force or the [National Policing Improvement Agency] Technical representative stated in this Agreement".

It was not within the scope of this inspection to explore in detail the nature of Cafcass' responsibilities to children or the legal obligations under which the organisation is expected to act.

We consider that the working practice as described to us was incompatible with the relevant term in the *Supply Agreement*. On the assumption that Cafcass' access to the PNC is to continue, there needs to be amendment either to the working practice or the *Supply Agreement*.

Does the organisation comply with its Security Operating Procedures?

We found that Cafcass 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.[13] During the inspection we examined the relevant training records. These were extensive and satisfied us that all Cafcass' PNC users had completed accredited training delivered by NDI Technologies.[14]

Physical security

A further requirement of the *Security Operating Procedures* is that the PNC terminals must be located in a secure building.[15]

We found that the organisation's PNC terminals were located in an office within the Cafcass headquarters building. All staff within the office were authorised to access the PNC. Access to the building was by a locked door and access through internal doors was by swipe card. Visitors to the building were required to be accompanied at all times.

Internal audit

We found that Cafcass had software known as 'PNC Guard and Transaction Analyser' installed on its PNC terminals. This software, which was approved by the Home Office, was used in order to carry out automatic audits on the PNC

[13] *PNC Security Operating Procedure Version 0.*7, Cafcass, February 2015, paragraph 4.1.

[14] The College of Policing is responsible for the accreditation of PNC training providers.

[15] *PNC Security Operating Procedure Version 0.*7, Cafcass, February 2015, paragraphs 3.8 to 3.10 inclusive.

transactions carried out by Cafcass staff. The software randomly selected PNC checks for audit and sent emails to the originators of the checks and the PNC operators, requiring them to explain in writing why each PNC check had been carried out.

Due to the high volume of checks carried out by Cafcass (more than 10,000 each month), this system made the audit process significantly more efficient than the manual equivalent which was in use in most of the other non-police organisations we have inspected.

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

- Audits will be conducted weekly to ensure PNC checks are being requested for the proper purpose as outlined in the *Supply Agreement*.[16]
- The audits will be completed by the Cafcass PNC auditor. The auditor will be independent of the office manager and PNC users. A clear trail of why the check was requested, by whom and how it was completed on the PNC terminal will be completed. At least 10 percent of all requests will be checked.[17]

In relation to the first requirement, we saw the PNC Guard and Transaction Analyser system in operation and how it automatically selected cases for audit. It did so on a weekly basis. The system met all the requirements for audit set out in the *Security Operating Procedures*.

In relation to the second requirement, we examined the organisation's audit records and found that 10 percent of all PNC checks carried out were audited. We checked a sample of the audits and found them to be accurate and correctly carried out.

All audits were sent to the manager for review, which we considered to be good practice.

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.

[16] *Ibid.*, section 11.

[17] *Ibid.*, section 11.

Conclusions

Level of access

We conclude that Cafcass needs direct access to the PNC and that the absence of a current *Supply Agreement* is a serious matter that should be remedied at the earliest opportunity.[18]

Taking into account the purposes for which Cafcass needs PNC access, we conclude that the level of access specified in the expired *Supply Agreement* is sufficient for the business needs of the organisation. However, because of the incompatibility between the *Supply Agreement* and Cafcass' working practice, we advise the Police Information Access Panel to review the *Supply Agreement*, amend it if necessary, and then satisfy itself that Cafcass will comply with the terms of the *Supply Agreement* in future.

Compliance

The comprehensive training records, the satisfactory physical security arrangements, and the level of internal audit coverage using the PNC Guard and Transaction Analyser system, lead us to conclude that the Cafcass has been complying with the requirements of its *Security Operating Procedures*.

Efficiency and effectiveness

We conclude that, but for the areas for improvement described above, Cafcass is making efficient and effective use of the PNC.

[18] Following this and other PNC inspections, we understand that the Home Office replaced *Supply Agreement*s with documents entitled *Agreement for the Supply of PNC data via Direct Access* and *Memorandum of Understanding Regarding the Supply of PNC data via Direct Access*. We were informed that one of the latter documents was issued to Cafcass on 9 February 2016.