Use of the Police National Computer by non-police organisations

A pilot inspection of Royal Mail Group Security

May 2016

ISBN: 978-1-78655-134-4

www.justiceinspectorates.gov.uk/hmic

Contents

Introduction

This inspection resulted from a recommendation by Sunita Mason in her 2011 review of the criminal records regime in England and Wales where she stated:

> "...once access has been granted, it is vital to have effective auditing arrangements to check it is being used appropriately and in line with the agreed conditions. HMIC has strong expertise in this area and their audit role should be extended to cover all Police National Computer (PNC) users, with the users agreeing to meet the cost of the audit."

This review is an inspection utilising the protocol and methodology adopted for this process.

Organisations are prioritised for audit using an assessment based upon issues that increase the risk of non-compliance, for example agencies with high numbers of PNC users based at multiple locations and/or update privilege.

Royal Mail Group (RMG) Security was selected because of the organisation's wide range of access codes, the volume of transactions and update authorisation.

HMIC would like to thank the Royal Mail Group Security staff for their co-operation with this inspection.

Agency Profile

In October 2013, Royal Mail floated on the London Stock Exchange as the principal trading entity of Royal Mail plc. Royal Mail Group Limited includes UK Parcels International and Letters (UKPIL) which comprises the Group's UK and international parcels and letter delivery businesses operating under the 'Royal Mail' and 'Parcelforce' worldwide brands.[1]

Royal Mail Group (RMG) Security is based in London and has offices throughout the country. The prosecution's office is in Leeds. The organisation investigates all criminal occurrences that have an impact upon Royal Mail. Royal Mail should not be confused with the Post Office which is a different company.

RMG Securities concluded 295 successful prosecutions in 2013/14, a slight reduction on the previous year. This is due to individuals being prosecuted by other agencies. Additionally RMG Security has had notable successes in recovering criminal losses, both as sanction and deterrent. Since its introduction RMG has

[1] Royal Mail website

taken full advantage of the Proceeds of Crime Act and has developed two accredited financial investigators. In 2013/14 RMG Security recovered a total of £1.22m in losses and costs, compared to £295k in 2012/13.

Use of the Police National Computer (PNC)

RMG Security has had access to and made use of criminal record information since 1975. Initially managed through local head postmasters and local senior police officers, the process then involved a member of the collator's office, now the intelligence team, physically attending Scotland Yard. A telephone contact process existed for urgent investigation checks. In the mid-1990s Post Office Security & Investigation Services were granted permission to put PNC terminals directly into the intelligence team office, then based in Croydon and all checking, both for investigation and recruitment, was undertaken in secure conditions by security-cleared personnel. Access is currently authorised by a memorandum of agreement with the former Police Information Technology Organisation (PITO), now Home Office, dated April 2005. PNC data management is currently undertaken by members of the security intelligence team based in Royal Mail premises in Battersea, London.

The agency was last inspected for compliance and audit by the National Policing Improvement Agency (NPIA) in July 2009. The inspection found the PNC management regime was good. There were two minor areas on concern in relation to printouts and retaining copies of documents for auditing. There are no outstanding actions from this inspection. A copy of the report is attached at Annex 2.

Royal Mail Group Security has direct view and update access to the PNC, which was tailored to meet the needs of the agency. The allowed computer access codes are detailed in Annex 3. Access was authorised by the PNC Information Access Panel (PIAP) and is regulated by Security Operating Procedures (SyOPs).

Methodology

A full inspection was carried out covering: Leadership; Policy & Strategy; People; Partnerships & Resources; Processes and Results. For the purpose of comparison national data supplied by the Home Office has been used to compare performance with other agencies. Any variations from what appears to be the norm highlights differences in working practices.

The first stage of the inspection involved the agency providing HMIC compliance auditors with documentation supporting their adherence to the protocols. This was followed up by a visit to the agency during which HMIC interviewed key staff. The visit to the agency also incorporated the final stage of the inspection, which was based upon reality checks. The reality checks included reviewing the results of data

protection audits conducted by the agency and checks against groups of practitioners.

It was encouraging to discover the way in which the agency has a clear understanding of the limitations and responsibilities of data management in respect of PNC data. There is also an active and verifiable data audit regime, which is not only understood by its managers, but also by personnel with day to day access to PNC data.

There are a number of recommendations relating to minor issues which are detailed in Annex 1.

Using the evidence gathered during each stage of the inspection, this report has been produced based upon the European Foundation of Quality Management (EFQM) format.

1. Leadership

1.1. The RMG Security is a national organisation with its headquarters in London. Tony Marsh leads as Group Security Director with Roger Duckworth heading the Security Intelligence Team.

1.2. Day to day responsibility for PNC usage lies with Elizabeth Critchley (Lead Intelligence Transaction Manager) who reports to Stephen Welch (Senior Security Transactions Manager). There is a clear line of responsibility from the PNC Manager, to the senior officer in the company there is no requirement for a specific strategic PNC management group.

1.3. Elizabeth Critchley supervises five PNC operators who provide business hours access to PNC for the organisation.

2. Policy and Strategy

The organisation has supplied the following documents:

2.1. Policy – At the start of this inspection HMIC found that RMG Security was using PNC in accordance with a SyOps (6.2) dated November 2014. RMG Security has recognised the need to update this document and have produced, but not yet finalised, an updated version. Although further work is required to bring it to the required standard, (for example it does not reflect the new government security marking scheme) it is clear there is a commitment to updating it.

2.2. Organisational structure – A comprehensive chart of the organisational structure has been examined. The structure clearly defines the lines of responsibility for any escalation issues.

Investigators are based in offices throughout the country. The Prosecutions Office is based in Leeds.

2.3. Audit – No document was submitted specifically relating to audit but the process has been described in full (See 5.21).

2.4. Training – Training material for PNC operators have been supplied by PNC national training. Training for operational personnel has been supplied and is mainly fit for purpose the exception being in relation to the timeliness of submissions which is addressed at (5.10 et al).

2.5. Development – All documents are comprehensive and fit for purpose. Subject to the above, the SyOps is relevant and current; the audit is an ongoing effective process which is supported by training where necessary. There is a clear line of responsibility from operational personnel in the control centres and on patrol through their line manages to the PNC manager who reports to national management.

3. People

3.1. The PNC staff at RMG Security work from the central London offices. From here a PNC facility is provided to all the investigation and prosecution personnel. While normally PNC is available during normal office hours, staff do start work early if required to support a particular operation.

3.2. All staff with direct access to PNC have been trained by PNC National Training.

3.3. The staff with direct access to PNC (described by the organisation as 'Intelligence Transaction Administrators') are trained for enquiry and update transactions. Authorisation includes access to the persons and vehicle databases.

3.4. Typically a request for a PNC check is made in respect of a person or vehicle. The updating of prosecution information including case results is also monitored. The organisation has supplied a document detailing how PNC should be accessed and updated. The document is comprehensive and covers most eventualities for officers involved in crime enquiries.[2]

3.5. All members of staff interviewed both input and operational demonstrated a good understanding of the potential of PNC and their responsibilities for its correct use.

3.6. Investigating officers understand the potential of PNC and use it to good effect.

[2] *Reporting Offences to the Police National Computer (including the Simple Caution Process)*, Royal Mail, 2014, version 1.0.

4. Partnerships and Resources[3]

4.1. At present Royal Mail Group maintains a team of over 215 security experts and inspectors, criminal investigators and prosecuting lawyers. It invests in excess of £14m per year in the staff and support costs for this function, with further capital investments that can exceed £10m in year.

4.2. RMG Security's Criminal Investigations Team raised 712 investigations across the group in 2013/14, resulting in a total of 506 individuals being dealt with for crimes committed against Royal Mail Group. 306 Royal Mail employees were identified as offenders last year, compared to 409 the previous year, the reductions coming mainly in the theft and Postal Services Act categories, however 36 Parcelforce employees were identified, compared to only 16 the previous year. 177 outsiders were identified for offences against Royal Mail, compared to 232 the previous year, of these 115 committed offences of fraud, down 11 on the 126 from 2012/13.

4.3. Some 295 successful prosecutions were concluded in 2013/14 compared to 322 in 2012/13. The reduction in conviction numbers stems entirely from individuals dealt with and prosecuted by other agencies, while Royal Mail-led prosecutions increased from 264 to 268 over the last two years. RMG Security has taken full advantage of the Proceeds of Crime Act and has developed two Accredited Financial Investigators. In 2013/14 RMG Security recovered a total of £1.22m in losses and costs, compared to £295,000 in 2012/13. RMG attempts to recover customer losses as well as its own and will usually reimburse domestic customers affected by proven theft of or from the post.

[3] Summarised from RMG document 'Notes for Home Office briefing on PNC vetting access – 25/06/2014

5. Processes

5.1. PNC individual checks can be conducted for the following reasons:

- To assist investigators with the investigation of specific criminal offences against Royal Mail Group.
- To assist investigators with risk assessments for Health and Safety purposes.
- For Health and Safety purposes, to conduct relevant checks on persons resident in house/premises that needs to be searched.
- Obtaining the previous convictions of alleged offenders, and witnesses who have provided a written statement, in cases being prosecuted or under active consideration for prosecution. These checks must be requested via Prosecution Support Office (PSO).
- For court purposes, where Royal Mail Group is the prosecuting body.
- To establish the outcome of a Police prosecution where the offence is against Royal Mail. These checks should be submitted by the Prosecution Support Office.[4]

5.2. PNC vehicle checks can be conducted for the following reasons:

- To identify the registered keeper of a vehicle that is suspected of being involved in criminal activity against Royal Mail or associated business units.
- To identify registered vehicles at an address that is associated with a known suspect, who is suspected of being involved in criminal offences against Royal Mail Group.
- To assist with the gathering of intelligence of vehicles used in crimes against the business.
- For Health and Safety reasons – Where the vehicle is to be search, whether as a suspect vehicle or as part of an ‘open enquiry’.

5.3. RMG Security forwards messages relating to PNC by use a computerised system which is used to record, store and finalise all operational messages. This seamless inter-operability ensures the exchange of timely, accurate data. Requests for PNC checks are sent on a pre-defined GS208 form (accessed

[4] Royal Mail Group 2014 Access to PNC Data for Intelligence Purposes v.9.0 November 2014

from the ‘Share Point’ computer system) and must be authorised by a team leader. Any available PNC operator can process the request and respond in the same way. This provides a clear audit trail for PNC enquiries and is good practice.

5.4. Upon receipt the request is checked by the PNC operator and the transaction completed. The result of a positive outcome is printed, scanned, password protected and emailed back to the enquirer. The documentation is retained for a few days should there be any query. Forwarding the result of the original enquiry risks the information being out of date.

5.5. Upon receipt by the OIC the PNC printout is printed and the message deleted. The PNC result is attached to the prosecution file and managed in compliance with the procedures relating to that file.

5.6. PNC requests must be referred to the investigation file reference which is issued by the Prosecutions Support Office at the commencement of the enquiry. This maintains a link from the enquiry to the PNC check which can be audited. It is good practice.

Recommendation 1

Immediately – The result of a PNC check should not be retained. Any subsequent request should be treated as a new enquiry.

5.7. While the email method referred to above is the prime system for PNC checks there have been in the past occasions when the results have been forwarded by special delivery or facsimile.

5.8. Both these methods have inherent weakness, particularly the facsimile method as there is potential for misdialling and machine reliability problems. Any facsimile print is only as secure as the premises and can be viewed by unauthorised personnel.

Recommendation 2

Immediately – The practice of sending PNC results by special delivery and facsimile be discontinued.

5.9. All staff interviewed are aware of these criteria and compliance is strictly monitored by the PNC manager. A review of audit returns carried out by HM Inspectors indicated that compliance is good. The agency is satisfied that this level of access is sufficient for their purposes.

5.10. Since March 2014 the organisation has updated PNC in its own right. It has been authorised to create Arrest/Summons reports on PNC. It is also responsible for recording the subsequent court results.

5.11. To guarantee the accuracy of PNC records, police forces are required to adhere to strict timeliness criteria for the creation and finalisation of these records. Full details of RMG Securities performance is detailed below (See (5) Results).

5.12. Accepting the fact that, compared to a police force, the numbers are low and the subsequent percent extrapolation suggests very poor performance, the organisation is consistently failing to achieve the standard over twelve month period.

5.13. It is possible that the agency is not aware of the standards. It is also a matter for PIAP as to whether non-police agencies should be required to adhere to them.

5.14. HMIC take the view that the timeliness standards ensure consistent, timely PNC data and the organisation should adhere to them.

Recommendation 3

Within three months – RMG Securities commence a dialogue with HMIC and PIAP with a view to achieving national timeliness standards.

5.15. The organisation has clear instructions to Investigators in charge (IIC) relating to the need to notify the commencement of proceedings.

5.16. The PNC data form GS090 must be submitted for any RMG Securities-led prosecution and the requirement for the collection biometric data is set out in some detail for the various prosecution scenarios.[5]

5.17. The document clearly identifies when and how biometric data should be collected. It has been suggested that the 'Cellmark' operators obtain fingerprints and DNA sample on behalf of the organisation prior to appearance at court.

5.18. Where the fingerprints and DNA have not been taken a template letter is available requesting that the local police assist in obtaining them.

5.19. It is accepted that, particularly where the offenders are employees, their identity is known with some certainty. However, anecdotal evidence suggests that fingerprints and DNA are not being taken in a significant number of cases particularly when the police do not respond to requests.

5.20. The taking of samples has on many occasions connected apparently unrelated patterns of offending, an opportunity not to be missed. Conviction

[5] RMG Securities document 'Reporting Offences to the Police National Computer (Including the Simple Caution Process).

data not supported by biometric data can and has been challenged at a later date.

Recommendation 4

Within three months – The organisation review the procedures and practices supporting the collection of biometric data particularly in relation to obtaining the cooperation of the police.

5.21. Auditing is by the Lead Intelligence Transaction Manager who prints off a weekly transaction log for authorised staff. This is compared to the supporting paperwork and 10% of the logs are checked. The transactions are numbered consecutively and a gap is highlighted and queried. The transaction is checked as being correctly authorised.

5.22. To support investigating officers working out of the office there is a facility for urgent checks to be carried out in response to a telephone request. The audit process identifies these and ensures that the paperwork was submitted.

5.23. The auditor's work is checked by her line manager.

5.24. No abuse of PNC has been discovered, any non-compliance tends to be related to administrative errors. This method of regular risk based auditing is good practice.

5.25. During the months leading up to Christmas the organisation recruits approximately 30,000, casual staff to deliver the Christmas mail. The recruitment process requires the screening of the applicants for previous convictions; this is normally done by application to the Disclosure and Baring Service, Scotland (DBS). To ensure a timely response Royal Mail has a service level agreement with DBS.

5.26. In October 2013 it was apparent that, due to the volumes and procedures relative to the DBS, applicants would not be screened in time. An approach was made to PIAP to allow the PNC bureau to undertake this task. Permission was granted and a potentially unacceptable situation was avoided. The authorisation was a temporary measure.

5.27. In an effort to formalise the procedure, in June 2014 RMG applied to PIAP for the facility to screen employees to be made permanent. This was refused and RMG appealed. The appeal was refused on the grounds that it would set a precedent for other authorised users and circumvent the existing procedures for access via the DBS.

5.28. In October 2014 the transaction statistics suggest that the volume of PNC transactions increased only slightly. It is apparent that the Royal Mail and DBS

have worked towards a solution to the problem of high seasonal volumes and the use of PNC for this purpose is negligible.

5.29. Interviews with operational investigators suggest a good understanding of PNC's potential. Examples cited are its use in the preparation of Health and Safety assessment of target dwellings, particularly in relation to firearms held by occupants. Another example given relates to the use of VODS to identify whether a suspect has access to other vehicles which may be used for the removal or storage of stolen property. This level of awareness is good practice.

6. Results[6]

6.1. This relates to the recording of the commencement and conclusion of proceedings.

Commencement of Proceedings

6.2. The national standard[7] is that the commencement of proceedings, recorded by the creation of an Arrest/Summons record on PNC, must be within one day in 90 percent of the event. The event could be an arrest or the date a decision is made to issue process. The Arrest/Summons record is referred to as an 'Impending Prosecution' (IP). The IP will remain 'live' until the proceedings are concluded. Proceedings can be concluded in many ways for example the decision may be made not to continue the prosecution or the person may be dealt with at court or be cautioned.

6.3. A high number of IP's may indicate that the finalisation of proceedings is not being recorded in a timely manner. It is considered good practice to develop an audit regime for IP's to ensure they are still valid and finalisations have not been missed.

2014	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Number of IPs created	21	18	22	11	15	13	10	7	16	9
Number of IPs outstanding	17	30	40	43	46	49	49	44	50	50
% In One Day	0	0	0	0	0	0	0	0	0	0
Days to achieve 90%	4	37	120	58	229	311	122	323	307	201

[6] This section relates to 'recordable offences'. These are all offences that carry the option of imprisonment and some 50 other, non-imprisonable offences listed in the National Police Records (Recordable Offences) Regulations 2000, as amended.

[7] Currently under review.

Conclusion of Proceedings

6.4. The national standard for the recording of the conclusion of proceedings is that 75 percent must be recorded within 10 days of the event. The event can be the conclusion of court proceedings or any other disposal.

6.5. The computerised resulting link between magistrates' courts and PNC has in recent years transferred responsibility for this standard to the lower courts. Occasionally the computerised link fails which may happen for a number of reasons, usually because the original charge has been removed/deleted/modified and the results cannot be 'mapped' across. Problems are exacerbated for non-police prosecutors because, as a result which cannot be mapped defaults to the local police, they are dependent upon the police taking the correct action. There is however no computerised links with the higher courts, responsibility for updating court results on PNC remaining with the prosecuting authority.

2014	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
Total Number of Disposals	0	0	2	1	2	5	3	8	4	1
% Entered in ten days			43	43	21	9	81	16	43	0
Days to Achieve 75%			12	12	46	57	9	46	12	28

Annex 1 – Summary of recommendations

Recommendation 1

Immediately – The result of a PNC check should not be retained. Any subsequent request should be treated as a new enquiry

Recommendation 2

Immediately – The practice of sending PNC results by special delivery and facsimile be discontinued.

Recommendation 3

Within three months – RMG Securities commence a dialogue with HMIC and PIAP with a view to achieving national timeliness standards.

Recommendation 4

Within three months – The organisation review the procedures and practices supporting the collection of biometric data particularly in relation to obtaining the cooperation of the police.

Annex 2 – PNC users compliance audit report

Royal Mail letters security – 21 July 2009

RMLS staff: Michael St. John and Liz Bond

Compliance Auditor: Roger Dale

1. Security Operating Procedures

Observation

Michael confirmed that the current version of the Security Operating Procedures (SyOPs) is 4.8, dated September 2008, but Liz is in the process of revising the document and had sent me a draft copy of version 4.9.

A hard copy of the SyOPs is kept in the secure room and an electronic copy is held on the shared drive. So, the operators have easy access to it when required.

I saw evidence of the signed Proper Use Declarations and the number of signed declarations tallied with the number of user accounts currently defined to the PNC.

It is important to remember to that the Proper Use Declarations need to be re-signed when the SyOPs are revised and re-issued.

Action required

RMLS demonstrated good practice in respect of controlling their Security Operating Procedures and corrective actions are not required.

2. Control of Userids

Observation

Prior to conducting this audit, I obtain a list of the user accounts currently defined to the PNC. The list from the PNC matched the list of current users and auditors and the last used dates indicate that all accounts are in current use.

We discussed the importance of all users logging on regularly to check the last used date and time and to change their password, thus maintaining control of their account. Liz stated that the reserve auditor is an irregular user but already follows the above guidance on maintaining control of his account.

Liz stated that she uses the range of #S transactions to monitor usage of all the accounts and does so weekly. I saw the current PNC5 form, which lists the current users and has a history of managing old accounts.

Action required

RMLS demonstrated good practice in respect of controlling their user accounts and corrective actions are not required.

3. Entering the system (includes control of Secure ID token and server password and individual password control)

Observation

Liz confirmed that all users are required to check the last logon date and time whenever they access the PNC.

RMLS have two Secure ID tokens. One is retained for contingency purposes. Both tokens are stored in the secure room. The main one is held in a drawer by the main PNC terminal and the other is held in the safe in the room. While non-PNC staff who have access to the secure room could get access to the main token, they would still need to know a valid user account and password to access the PNC and there would be a strong chance of their being seen using the terminal. So, the current storage process is appropriate.

Action required

RMLS demonstrated good practice in respect of controlling their access to the PNC and corrective actions are not required.

4. Training

Observation

Liz confirmed that all users are fully trained before being allowed to access the PNC and that all training is provided by the NPIA.

Action required

RMLS demonstrated good practice in respect of the training requirements and corrective actions are not required.

5. Physical location

Observation

RMLS currently have six PNC terminals and one printer housed in a secure room within the Security Intelligence Transaction Team area. Access to the room is controlled by programmed identity cards and access is only granted to PNC-trained staff and certain vetting staff. Visitors to the room must be signed in and out.

Action required

RMLS demonstrated good practice in respect of physical security and corrective actions are not required.

6. Print handling

Observation

Liz confirmed that a printout is taken whenever there is a 'hit'. Each print is stamped 'RESTRICTED'. For vetting requests, the print is put on the relevant file, which stays on the premises until it is destroyed. For investigation and witness checks, the original print is sent to the requestor in a double cover package via the Royal Mail Special Delivery, which provides a full tracking service. Rarely and if the matter is urgent, the print is sent by fax to the requestor following the faxing guidance set out in the Security Policy Framework. All prints are copied and the copies retained for audit purposes.

Action required

1. Despite following approved guidance for the use of fax, there is still a risk of the data ending up in the wrong hands. So, I advise that fax should not be used except in the most urgent of cases.

2. I cannot see any value in taking a copy of the printout for audit purposes. Indeed, taking copies increases the risk of compromise. So, I request that this practice cease.

7. Incident Handling

Observation

Liz confirmed that there had not been any information security incidents since the last compliance audit. So, we discussed incident management in theory, the need to differentiate between breaches of policy and incidents and when to notify the NPIA.

Action required

N/A

8. Operational process

Observation

In respect of vetting, the applicant completes and submits the Security Questionnaire, which then forms the source document. The operators work directly from the SQ. Therefore, there is very little likelihood of anyone being able to insert the name of someone in whom they have a personal interest.

In respect of witness checks, the requestor completes form GS202 and sends it to the SITT by post. The form is authorised by a senior staff member at source, thus minimising the risk of the requestor making an illegal search. The operators work directly from the forms.

In respect of investigations, the requestor completes form GS208, which is authorised at source, and sends it electronically to the SITT group mailbox. The operators print the form from the group mailbox and work directly form it.

Occasionally, when operationally imperative, the requestor will make the request by telephone. In these cases, the operator will complete form GS208 at the time and undertake the check. After making the check and returning the results to the requestor, a copy of the form is sent to the relevant authorising manager to confirm the appropriateness of the check. There is a process for ensuring that the manager replies to the request for confirmation. Liz was confident that the operators will always recognise the requestor and that there are sufficient safeguards to avoid being tricked into doing a check for an unauthorised person, e.g. a journalist.

Action required

RMLS demonstrated good practice in respect of their operational process and corrective actions are not required.

9. Auditing

Observation

Liz explained that she is the main auditor but there is a second, trained auditor to cover any periods of absence. Until Liz returned in January, audits were being conducted monthly, which contravened the requirement in the SyOPs. Auditing is now being done weekly.

Liz uses the range of #S transactions to monitor the status of the user accounts. She uses the #TE transaction to list all the transactions done by each user for the audit period and prints the resulting logs. Liz selects at least 5% of the transactions to be fully audited but also checks the operators' login and log out times to see if they match the entries on the PNC1 form, the times between transactions and the sequential numbering. Discrepancies are noted and queried with the operator

concerned. The operators are required to sign Liz's audit report to confirm they accept the findings.

For the 5% full audit, Liz checks the source document to make sure the target name tallies with that entered on to the PNC. At the same time, she checks that the request form has been completed correctly.

The operators are instructed to notify Liz as soon as possible if they have made a mistake during a logon session.

Michael and Liz meet regularly to discuss the process and look for enhancements.

Action required

RMLS demonstrated good practice in respect of local auditing and corrective actions are not required.

Annex 3 – Allowed PNC codes

BB	Bulletin Board Enquiry
CL	Clear Data from Screen
LG	Securedial – Restricted Names Access 2
MM	Display Transaction Menu
NE	Names Enquiry
NU	Names Update
NV	Names Verification
NX	HMRC etc. – Names Enquiry
NZ	Other Gov Dept Names Enquiry
QC	Court Enquiry
QS	Force/Station in Detail Enquiry
QV	Select DAF reports and On-Line Verification
RP	Reset Printer
SD	Show User ID/User Groups
SE	Show User ID Information
SG	Maintain User-Group Membership
SP	Reset Password
SU	List Unused User ID’s
TE	Transaction Log Search

VF	Full Postcode Search
VK	VRM Basic Enquiry
VP	Partial VRM Enquiry
VQ	Display Vehicle Tables
VR	View VODS Results
VS	Initiate On-Line VODS Search
XX	Log Off

Usage – 12 months to December 2014

	#BB	#CI	#LG	#MM	#NE	#NU	#NV	#NX	#NZ	#QC	#QS	#QV	#RP	#SD	#SE	#SG	#SP	#SU	#TE	#VF	#VK	#VP	#VQ	#VR	#VS	#XX	Total
Jan			231	2				16										2	43	38	9					3	344
Feb			232			2	1	20											56	54	22					7	394
Mar			182	1		96	12	9		14	1	2							58	33	8	1				30	447
Apr			188	2		112	2	15		2									50	29	10					31	441
May			196	1	84	159	2	22	1	15									74	23	9					46	632
Jun			160		9	68		20											32	38	15					36	378
Jul			126	1		115		17		2									35	37	9			3	1	40	386
Aug			155			80		15		16									27	44	25			3	1	24	390
Sep	1		163			74		10		3									52	37	16					42	398
Oct	1		341		10	77		15		1									42	38	25					28	578
Nov			98		3	67		11											35	21	10	1				30	276
Dec			105			46		20		1									23	29	17	6		5	2	23	277

Source for allowed codes NDI. Highlighted items are not recorded by NDI.
Data from Hendon Data Centre.

Annex 4 – Glossary

DAF	PNC Daily Activity File - a summary of activities produced to assist audit.
DBS	Disclosure and Baring Service. The Scotland based agency created to screen personnel for criminal history.
EFQM	European Foundation of Quality Management
IIC	Investigator in Charge
NPIA	National Policing Improvement Agency created in April 2007 and subsumed in the Home Office in October 2013.
PIAP	PNC Information Access Panel – a panel of experts chaired by a chief police officer tasked with reviewing requests for access to PNC and stipulating restrictions where access is allowed
PITO	Police Information Technology Organisation. Originally responsible for PNC the organisation was subsumed in the NPIA on 1st April 2007
PNC	Police National Computer
RMG	Royal Mail Group
SyOPS	System Operating Procedures – a document setting out the way in which the agency can use PNC
UPKIL	UK Parcels and International Letters