Post Office Ltd PNC Security Operating Procedures

Aug 2012 – Version 1.1

Contents

Revision History

Status	Live
Issue Version	1.1
Owner	John Scott
Authors	Mark Dinsdale
Enquiries	Mark Dinsdale, John Bigley or Dave Pardoe
Release Date	
Document Privacy	Internal Information- Post Office – Confidential

Document History

Version	Status	Reason and Changes	Author	Date
0.1	Draft	Inception of Document	Mark Dinsdale	30 October 2012
0.2	Draft	First corrections from Roger Dale	Mark Dinsdale	16 January 2012
1.0	Live	Second corrections from Roger Dale	Mark Dinsdale	30 January 2012
1.1	Live	• Removal Appendix C (GS202) and associated instructions, • Removal of 9.8.3 (vehicle checks, contradicts earlier vehicle type requests & subsequent clarification from Clare Chamberlain & expanded 9.1 for clarity • Re-named teams for consistency, changed font • Realigned Information Security standards • Changed discipline code to Conduct Code to align with POL standards • Removed sharing agreement to Royal Mail & reference to associated business units • Clarified accidental discloser • Additional Appendix added	Mark Dinsdale	28 August 2012

Queries about this document should be addressed either of the following:-

Mark Dinsdale Security Team Post Office Ltd 148 Old Street LONDON EC1V 9HQ mark.dinsdale@GRO GRO	John Bigley Security Team Post Office Ltd 148 Old Street LONDON EC1V 9HQ john.bigley@GRO GRO
Dave Pardoe Security Team Post Office Ltd 148 Old Street LONDON EC1V 9HQ dave.pardoe@GRO GRO	PNC Appointment Information.assurance@GRO

Glossary of Terms

ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers of Scotland
ACRO	ACPO Criminal Records Office
AUP	Acceptable Use Policy
CD	Compact Disc
DVLA	Driver and Vehicle Licensing Agency
GPMS	Government Protective Marking Scheme
HDC	Hendon Data Centre
NIS	National Identification Service
NDA	Non-Disclosure Agreement
NPIA	National Policing Improvement Agency
NPIA – ICTLP	National Policing Improvement Agency, Information Communication Technology Learning Programme
Operator (s) –	Post Office Ltd PNC Computer Operators
PNC	Police National Computer
POL 208	Internal PNC request form
Security Manager	Post Office Ltd Security Manager
SyOps	Security Operating Procedures
Taskforce	Post Office Ltd Risk Reduction Surveillance / Support vehicle
USB	Universal Serial Bus

1. Introduction

Introduction to the Police National Computer (PNC)

1.1 The Police National Computer is a national database of information available to all police forces/agencies throughout England, Scotland, Wales, Northern Ireland, the Isle of Man, the Channel Islands and British Transport Police.

1.2 The system is also available to other approved organisations and Government departments for specific purposes.

1.3 The following are some of the details held by PNC :-

- Personal descriptions
- Bail conditions
- Convictions
- Custodial history
- Wanted/missing reports
- Warning markers
- Pending prosecutions
- Disqualified driver records
- Cautions
- Drink drive related offences

Names

1.4 This file is maintained, mainly by the Police, together with the National Identification Service (NIS). It holds details of around 6,500,000 people who :-

- Have convictions for certain offences
- Are subject to the legal process, for example waiting to appear at court
- Are wanted by the Police
- Have had certain court orders made against them
- Are missing or found
- Have absconded from specified institutions
- Are disqualified from driving by a court
- Have a driver record at DVLA

Vehicles

1.5 This file mirrors the main details of the 47 million records held by the Driver & Vehicle Licensing Agency (DVLA) at Swansea. It includes :-

- ♦ Vehicle details
- ♦ Keeper details
- ♦ DVLA markers
- ♦ Police reports
- ♦ Vehicle insurance details

Important Considerations

1.6 Never

- X Leave your terminal logged on, no matter how short your absence
- X Perform unauthorised checks
- X Disclose PNC information to any unauthorised person
- X Allow anyone else to use your user ID
- X Disclose your PNC password to anyone
- X Demonstrate the PNC to anyone

1.7 Always

- √ Report any actual or suspected information breaches to the Security Programme Manager responsible for PNC
- √ Report any actual or suspected password security breaches to the Security Programme Manager responsible for PNC and immediately change your password.
- √ Ensure that your use of the PNC terminal is in accordance with the current POL PNC Security Operating Procedures (SyOps).

2. Legislation

2.1 PNC checks will only be made for the following purposes :-

- To assist Security Managers with the investigation of specific criminal offences against Post Office Ltd.
- In order to carry out risk assessments for health and safety purposes on identified occupants of premises/ places of residence / vehicles which are to be searched/ or subject of an operation carried out by Post Office Ltd as part of a criminal enquiry.
- 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 by Post Office Ltd.
- To establish the outcome of a Police prosecution where the offence is against Post Office Ltd.
- To identify the registered keeper of a vehicle that is suspected of being involved in criminal activity against Post Office Ltd.
- To identify registered vehicles at an address that is associated with a known suspect, who is suspected of being involved in criminal offences against Post Office Ltd.
- To assist with the gathering of intelligence of vehicles used in criminal offences against Post Office Ltd., for example suspected criminal activity against Cash & Valuables in Transit or Cash Centre Depots.

2.2 Accessing the PNC must comply with :-

- Section 29 of the Data Protection Act 1998, on the grounds of 'Public Interest' for the purposes of the prevention/detection of crime and the apprehension and prosecution of offenders.
- The Computer Misuse Act 1990.
- The Copyright Designs and Patents Act 1988.
- The ACPO Code of Practice for Data Protection.
- The 'Supply Agreement' between Post Office Ltd Security and NPIA.
- Post Office Ltd Security Operating Procedures.

2.3 For the purposes of Subject Access Requests, Post Office Ltd is not a Data Controller. The Data Controller for information held on the PNC is the Police Force or organisation that either created or last updated the particular record. NPIA act as a data processor.

2.4 It is criminal offence to perform 'fishing trips' on the PNC, for example conducting a PNC check on all individuals at a branch when only one person is suspected of a criminal offence.

2.5 Post Office Ltd Information Classification Standards to be adhered to in respect of PNC data:

2.5.1 CONFIDENTIAL Information that should only be shared with staff, agents and contractors who have a need to know. Any sharing of information with third parties, except disclosure for the purpose of disciplinary proceedings or disclosure during court proceedings, must be carried out under a Non-Disclosure Agreement (NDA). *(Almost all requested PNC data falls into this category (see 'Strictly Confidential' for exceptions) – Confidential Information is deemed to be of a sensitive nature and likely to cause damage following unauthorised disclosure.)*

2.5.2 STRICTLY CONFIDENTIAL Information that must be strictly controlled and limited to a minimal list of nominated individuals. The information owner is responsible for permitting access to information, controlling the list of nominated recipients and managing the disseminated information. *(- Strictly Confidential Information meets the classification standards of government departments, the security services or clients, or is deemed to be so sensitive that unauthorised disclosure would cause acute organisational damage*

3. System Security

Security of PNC Data

3.1 The PNC system is protectively marked as RESTRICTED in line with the Government Protective Marking Scheme. To comply with Post Office equivalent standards, 'Post Office – Confidential' will be used with all PNC requested data. In exceptional circumstances with approval from one of the Senior Security Managers, it may be deemed necessary to categories specific PNC requested data as 'Post Office - Strictest Confidential'. (See Section 2 for details of Post Office Information Security Standards)

3.2 It is important to remember that the PNC is not a Post Office Ltd computer system. This means that staff must exercise great care to ensure that abuses do not take place, such as using the computer for personal use or non-PNC related work.

3.3 ACPO have the right to withdraw the use of PNC from Post Office Ltd if there is a reason to believe it has been misused.

3.4 Two important rules are :-

- ONLY use PNC data for official use
- NEVER pass PNC data to those who do not need to see it, or discuss the data with such people.

3.5 The security arrangements for PNC are required to be compatible with those of ACPO. This is designed to protect :-

- Confidentiality – Ensuring that PNC information is disclosed only to authorised users for legitimate purposes
- Integrity – Ensuring there is no unauthorised access, deletion or alteration of the PNC data.
- Availability – Ensuring the PNC service is available when required.

3.6 When logging on to the PNC terminal, operators must always check the last logon date and time. These should correspond with the last session conducted by that user. If the date and time does not match (e.g. a logon was shown for yesterday and you were on leave that day) then this should be reported immediately to the Security Programme Manager responsible for PNC

3.7 PNC Grapevine Operators must not demonstrate the PNC to anyone not authorised to use the PNC system, without the prior approval of the NPIA.

3.8 The building where the PNC terminal is sited, is accessed controlled, with either personal access identification cards that provide controlled access, or via a manned reception during normal office hours. Beyond the reception, access is gained via personal swipe card access. The PNC terminal is then located within the inner room inside the alarm receiving centre, which is access controlled 24/7/365 by the inner secure room controller via siphon door access. Access to the small room the PNC terminal is located is secured when the PNC system is in use, thereby excluding all non PNC authorised persons.

3.9 The terminal must stay at its location as agreed at the inception of PNC access. Terminals can be moved when, for example, offices are relocated, but a member of the NPIA Information Assurance Team must be contacted to authorise the proposed location, prior to the move.

3.10 Under no circumstances must any form of removable media be used to download or upload data to or from the PNC or the terminal. Definitions of removable media include: floppy disks, any form of CD media, Zip disks, removable hard disk drives or similar and any form of solid state device e.g. USB pen drives.

3.11 Only pre-installed, authorised software may be used on the PNC terminal. It must not be used as a general office machine.

3.12 This document should be read and understood by all PNC users. This should be recorded using Appendix A and must be periodically re-signed within a time frame of no more than one year, which is being set at the end of July each year.

4. Access and Training

4.1 Only officially trained users may access the PNC. All training is undertaken through NPIA-ICTLP (the national Police trainers) or NPIA-ICTLP approved trainers. Informal training, such as shadowing an established user, without attending an official training course beforehand, is expressly forbidden.

4.2 All requests for PNC information, must apply using the dedicated internal information request form, currently titled POL208. All requests must be approved by the Authorising Manager which includes one of the Security Operations Team Leaders or a member of the Security Lead Team (which are all at least one grade above the PNC requestor).

4.3 PNC Authorising Managers, must on an annual basis read and abide by the 'PNC Authorising Managers Instructions Policy' to confirm all PNC requests are in accordance to the standards set out by the PNC Security Operations Manual. (See Appendix I). Frequency is set on the first occasion for September 2012, then by the end of July thereafter.

5 User IDs and Passwords

User IDs

5.1 The PNC User ID is unique to the operator. It determines the parts of the system the PNC Operators are entitled to access and identifies the operator to the system for audit purposes. Therefore, all operators must closely guard their password.

This still applies if a user is required to contact Hendon Data Centre; whilst a user ID can be revealed and indeed be guessed, the password must never be given to a third party, no matter how seemingly legitimate they may be.

PNC users are fully accountable for all actions undertaken with their User ID.

5.2 User IDs must be deleted when :-

- Employment is ceased
- The user moves to another department and no longer requires access
- Extended sick leave
- Maternity leave
- Secondment

Unfortunately, it is not possible to disable a user ID and reinstate it when the owner returns.

5.3 User IDs must be recorded on Appendix D

Passwords

5.4 Users will be allocated a password when they first gain access to the PNC. The system will prompt the PNC Operator to change the password upon first access.

5.5 PNC passwords expire at 45-day intervals after the initial logon and password change. The system will prompt the user to change their password ten days prior to the expiry date.

5.6 It is good practice to change a password prior to not requiring access for an extended period. This should counter any unnoticed security breach whilst the user is away due to leave or secondment.

5.7 The PNC enforces rules on password composition, these are :-

- Minimum of six, maximum of eight characters, which must be alpha-numeric (no spaces or punctuation symbols).
- No more than two consecutive identical characters
- A combination of letters and numbers
- Not the same as the user ID

It is also good practice to use passwords that are not easily linked to the PNC operator - for example, your birthday or car registration number.

5.8 If it is suspected that your password has been discovered, the password must changed immediately and then log a security breach with the Security Programme Manager responsible for PNC, who will in turn raise this with the NPIA. You must ensure that transactions conducted with the compromised user ID are audited to ascertain whether any breaches have occurred.

5.9 If you forget your password, it must be reset. Contact the Security Programme Manager responsible for PNC with the password request, completing Appendix E – Password Reset.

5.10 The PNC will bar a user ID if the corresponding password is entered incorrectly three times. The following message will be displayed if this has happened :-

'Too many unsuccessful log on attempts. This User ID is being barred'

If you attempt to log on after this has happened the following message will be displayed:-

'User ID is barred – Contact Security Administrator'

If this happens you should contact the Security Programme Manager responsible for PNC

5.11 If three invalid user ID attempts are made the terminal will be locked out. This is to prevent unlawful access if the physical security of the terminal becomes compromised. If this happens, the following message will be displayed :-

'Too many invalid log on attempts. This terminal is locked out'

If this happens you should contact the Security Programme Manager responsible for PNC

6. Security of PNC Prints

6.1 Scanned Prints: PNC prints are scanned and sent as an e-mail attachment to the relevant requesting Security Manager. The following form of words is sent with each e-mail that has a PNC print as an attachment. *'The PNC print attached to this e-mail contains "Post Office - Confidential" information and is provided on the understanding that it is managed with due regard to its' sensitive nature. The information provided should only be used to assist with the Post Office Ltd Security Manager specified by the requester and should not be shared outside the Security Team or appointed persons involved with the case.. The 'PNC print/s' attachment within this e-mail must be printed off immediately on receipt and the attachment then deleted. The printed copy must be securely filed with the relevant casework. Failure of an individual to delete a file or to forward a file without authority may be in breach of our PNC Security Operating Procedures and could instigate the conduct code (the level of misconduct dependant on severity of breach, which may lead to dismissal). If you have received this message in error, you must not view the attachment. Instead, please return the e-mail to the sender and delete this e-mail message from your system'*

6.2 The criteria and process detailed below are followed when scanning PNC prints to minimise the risks of compromising the PNC data.

- The image of the scanned print is deleted from the scanner / PC, immediately after attaching the scanned print to the relevant e-mail.
- The scanned print is deleted from the computer of the PNC operator dealing with the request, once the e-mail with the scanned print as an attachment has been sent.
- Once the e-mail with the scanned PNC print has been sent to the requesting Security Manager, the e-mail and attachment are deleted by the PNC operator from their computer.

6.3 In exceptional circumstances, where the scanning process is not appropriate and a printed copy is being sent by post or fax, the printouts must be protectively marked at 'Post Office - Confidential' in line with the Post Office Ltd Information Security Standards (see section 2).

- PNC prints must only be sent to Security Managers when necessary and when sending a scanned print is not an option. .

- All PNC prints must be marked 'Post Office - Confidential'

- PNC prints must not be distributed for vetting purposes.

- Data from PNC prints must not be disclosed outside the Security Team or appointed persons directly linked with the investigation, without first obtaining relevant senior manager approval, who will seek approval for disclosure from the National Policing Improvement Agency, if the request is considered appropriate.

6.4 If PNC prints need to be distributed as single items (as opposed to within dossiers/case files etc.) then the procedure detailed below should be followed.

- PNC prints must be sent double enveloped. The inner envelope should be sealed and marked 'Post Office - Confidential'. The outer envelope should be without protective marking and sent by Special Delivery.

- Faxes should only be sent in matters of extreme urgency and agreement obtained from one of the Authorising Mangers before doing so.

- If distribution is by fax: a known fax number and established contact should be used, additionally the recipient should be on hand. The fax number must be a recognised and official contact number. The image must then be deleted from the fax machine.

6.5 PNC Prints left lying around can be easily read by anyone entering the office and therefore give rise to accidental disclosure. If this happens, you have disclosed the data and, the conduct code may be instigated (level dependant on severity, which may include dismissal). If deemed an intentional disclosure then you may be liable to prosecution

7. Storage

7.1 All documents relating to PNC are protectively marked at 'Post Office – Confidential', as such, all documents should be treated in the same way as other RESTRICTED documents. For both government and non-government organisations this means protected by one barrier, e.g. in a locked container within a secure building.

7.2 The SecureDial token, PIN, if applicable and server password, if applicable, will be shared by all PNC terminal users. These items may be stored in one place so long as access is restricted to PNC terminal users.

8. Disposal

8.1 Documents marked at 'Post Office – Confidential' should be disposed of by tearing into pieces so that reconstitution is unlikely and deposited within the sensitive waste container or shredded.

9. Operational Procedures

9.1 The PNC terminal has been provided to facilitate in the investigation of internal Post Office Ltd incidents & potential criminal activity against Post Office Ltd as prescribed in section 2.1. All requests are made by members of the Security Team during the process of pulling final cases together prior to court appearances (although some cases may be closed and therefore not reach court) or potential criminal activity against Post Office Ltd. (for example potential criminal activity against Cash & Valuables in Transit or Cash Centre Depots).

9.2 For all **standard requests for PNC checks**, form POL208 must be completed, authorised and e-mailed to the 'Post Office Security' email box (then forwarded to Post Office Grapevine). It is important to ensure that all available details are entered on the form in accordance with the instructions contained on the POL208 form. The form must come from the e-mail account of a recognised authorising manager, which is either one of the Security Operations Team Leaders or a member of the Senior Lead Team i.e. a manager at least one grade above the requester, including the words 'I authorise this PNC check for (enter name of individual)' and include the original e-mail from the requester. (Names of all Authorising Mangers are kept with the PNC terminal).

9.3 For all **urgent PNC checks**, the Grapevine Team will accept requests made over the telephone as follows;

9.3.1 In all instances, full details must be provided and the reason for the check explained.

9.3.2 Details should include the name of the manager authorising the request.

9.3.3 The PNC information is telephoned back to the requestor using the recognised and official contact number.

9.3.4 The Grapevine Operator will complete the POL208 form and e-mail it to the Authorising Manager who must complete the authorisation boxes on the individual check form and return the form to the Grapevine Team e-mail address (and cc Post Office Security to enable consolidation of casework paperwork) within 5 working days in order to comply with Post Office Ltd Security Operating Procedures

9.3.5 The Authorising Manager should ensure the subject line is marked 'Urgent PNC Check' and the e-mail states 'I authorise PNC check for (enter name of individual)'.

9.4 When providing the reason for the request, it is important to bear in mind that our usage of the PNC is subject to external audit conducted by NPIA. A brief, but detailed reason should be given which will provide an external auditor (with no background knowledge of the case) an understanding of why the check was necessary. PNC requests must as a minimum contain the reasons for the request with evidence of some of the points listed in section 2.1 of this policy (i.e. purposes PNC checks are permitted for) to ensure the purposes of the request is to combat criminality against Post Office Ltd.

9.4.1 The Human Rights Act 1998 (HRA) stipulates the main considerations that must be taken into account before 'public authorities' can be allowed to interfere with the right to privacy. The operation of PNC is subject to HRA, which places an obligation on those using the powers to ensure that the check requested is fully and clearly justified. The Authorising Officer must ensure that any check meets HRA requirements and that use of the check is proportionate to the outcome being sought. Investigations should cause minimum interference with the rights of an individual and be necessary, justifiable, legal and proportionate.

9.5 PNC individual checks **cannot** be conducted for the following reasons: -

9.5.1 Checking the criminal record of individuals suspected of criminal offences where Post Office Ltd or appointed agent is not the victim or loser. For example, suspected use and/or supply of controlled substances such as drugs.

9.5.2 'Fishing trips' – Checking a number of individuals where there is no justified reason, for example, other individuals who could not have had access because they were not on duty or in the branch at the time of the incident.

9.5.3 Checking of individuals due to reports on their appearance or behaviour, for example, unsubstantiated suspicions.

9.6 For all vehicle PNC checks a POL208 form must be completed, authorised and e-mailed to the Post Office Security Team e-mail address. It is important to ensure that all details on the form have been completed and the instructions contained on the POL208 form followed. The form must be sent from the e-mail account of the authorising manager. (Including the words 'I authorise this PNC check for' enter the vehicle reg number and include the original e-mail from the requester).

9.7 For all **urgent PNC vehicle checks**, requests made over the telephone to the Grapevine Team are acceptable. Request should be made as follows:

9.7.1 Full details must be provided and the reason for the request given.

9.7.2 Details of the authorising manager.

9.7.3 The PNC information is telephoned back to the requestor using the recognised and official contact number.

9.7.4 The Grapevine Team will complete the POL208 form and e-mail the form to the authorising manager, who must complete the authorisation boxes and return the form using their own e-mail account to the Grapevine Team e-mail address within five working days (and cc Post Office Security to enable consolidation of case files)

9.7.5 It is important to ensure the subject line is marked 'urgent PNC check' and the e-mail states 'I authorise PNC Check for' enter vehicle registration'.

9.8 PNC vehicle checks **cannot** be conducted for the following reasons:-

9.8.1 'Fishing trips', i.e. – checking a number of vehicles when there is not any justified reason. This would also include the checking of vehicles, which may be parked near to a suspect address or where a criminal incident occurred, but there is no information/intelligence to suggest the vehicles are involved in criminal activity against Post Office Ltd

9.8.2 Vehicles not involved in criminal activity against Post Office Ltd.

9.8.3 To identify the ownership of vehicles in accordance with the proceeds of Crime Act, 2002.

9.9 PNC DISCLOSURE – INDIVIDUAL CHECK

9.9.2 All PNC data will be disclosed for an intelligence check – current convictions, impending prosecutions, spent convictions, cautions and warnings. A description of the individual will also be sent to the requestor.

9.9.3 Spent convictions are to be used for intelligence purposes only as these convictions are governed by the Rehabilitation of Offenders Act 1974. Under no circumstances should spent convictions be disclosed to unauthorised personnel. As these spent convictions are for intelligence use they should only be disclosed on a 'need to know basis' only within Post Office Ltd Security.

9.9.4 Where there is uncertainty as to whether the PNC result is that of the individual details provided, contact must be made to the requestor for verification. It is the responsibility of the Security Manager to check the PNC printout against the subject details in order to verify the information. If it transpires, a print-out is of the wrong person, the PNC print must be disposed of by shredding.

9.9.5 Under no circumstances must PNC printouts be circulated for disciplinary purposes.

9.9.6 PNC information must be treated in accordance with the Post Office Information Classification Standards, which under normal circumstances will be 'Post Office - Confidential).

9.9.7 Where there is a requirement for disclosure of PNC data to line management – for health and safety or conduct reasons then seek advice from one of the Senior Security Managers and they will give the relevant authority for disclosure if applicable. Consideration will be given to the legality, the public interest and the risks to the business when making a decision on disclosure. Authority must be obtained before any disclosure of PNC data.

9.9.8 If authority for disclosure has been given only current convictions can be disclosed. Under no circumstances should any other information be disclosed – Impending, spent, warnings, cautions etc.

9.10 PNC DISCLOSURE – VEHICLE CHECK

9.10.2 All PNC data will be disclosed for an intelligence check – Registered keeper details, vehicle details and any information in relation to the vehicle. The full vehicle PNC printout will be sent to the requestor.

9.10.3 PNC information must be treated in accordance with the Post Office Information Classification Standards, which under normal circumstances will be 'Post Office - Confidential).

9.11 OPERATING PROTOCOL

9.11.2 Ensure that all request forms are in accordance with 9.1 above. If there is any doubt refer the form to the relevant Security Programme Manager responsible for PNC

9.11.3 Following procedures detailed in accordance with operator training, log on to the PNC using personal user ID and password.

9.11.4 Refer to the PNC log on book (Appendix H / PNC1); ensure that the last log off time shown in the book matches the date and time shown on screen.

9.11.5 Refer any discrepancies to the relevant, Security Programme Manager responsible for PNC. The Security Programme Manager will refer where appropriate any discrepancies to the Senior Security Manager.

9.11.6 Enter the date and time of log on as shown on the PNC screen in the PNC Log on book (Appendix H / PNC 1). Take note of the last reference number used.

9.11.7 Commence the transactions requested. Each form to be given a consecutive reference number that must be entered in pen on the top of the form and entered in to the Origin string on the PNC.

9.11.8 Form POL208 must be endorsed as 'PNC No Trace' if a 'match' is not identified or marked 'NO RELEVANT INFORMATION' if a match does not provide any information. The date should be noted on the form next to the 'marking' and a copy of the POL208 form returned to the requester.

9.11.9 Where a 'match' is identified, a scanned copy of the full PNC print relevant to the check requested will be e-mailed to the requester. This will include spent convictions that are for intelligence purposes only and must not be distributed in any format outside of Post Office Ltd. No copies of the PNC print should be retained in the paperwork retained for audit purposes.

9.11.10 The process for dealing with, scanning, e-mailing and circulating PNC prints is documented in 'Section 6' of this document, 'Security of PNC Prints'.

9.11.11 In all instances, the POL208 form (source document) and email containing authorisation from the 'authorising manager' should be retained.

9.11.12 Irregular users are to check the log on sheet at the end of the month and if there has been no use, they will then log on. The Security Programme Manager will also identify irregular users as part of the weekly audit and issue reminders.

9.11.13 If at any time the operator has to leave the terminal then the normal exit procedures must be followed. The terminal must not be left on whilst the operator is away from the terminal NO MATTER HOW LONG.

9.11.14 When the operator has finished at the terminal then the normal exit procedures must be followed. The time that the operator has finished that session must be noted in the PNC Log on Book (PNC1) as well as the last reference number used.

10. Audit Procedures

10.1 Responsibility for audits rests with the Security Programme Manager responsible for PNC. However another PNC trained Security Programme Manager, may undertake this role as required.

10.2 Operators must not print their own PNC audit transaction log.

10.3 The above Security Programme Manager will not have access to the information on the PNC as a user but will be able to access the #TE transaction log, the #SP password change and the #SD List Security Files.

10.4 The frequency of audits will depend on the amount of transactions. If there is an average of more than 100 transactions per day, a daily audit will be required, reporting weekly. For less regular use, a weekly audit, reporting monthly will be appropriate.

10.5 The auditor will produce a #TE print of all transactions carried out during the audit period. This should include all periods over a day/week/month. For example, a weekly audit transaction report, the print should show the period Monday 0000 hours through to Sunday 2359 hours.

10.6 All current PNC operator transactions should be subject to audit.

10.7 The above Security Programme Manager conducting the audit should check the following:

10.7.1 That only current authorised users have accessed the PNC during the audit period.

10.7.2 That all user IDs are checked for PNC use even if on annual leave or known to have not accessed PNC during the period being audited

10.7.3 All sessions shown on the print are reflected by the entries in the PNC Log on book, including times and dates.

10.7.4 That all forms have a reference number annotated in ink at the top of the form.

10.7.5 That all paperwork is stored securely and no unauthorised disclosures have been made.

10.7.6 The #SU screen to ensure that only current authorised users are able to access the PNC.

10.7.7 The Appendix D – User ID's Log to ensure that details of present and past users is accurate and up to date. Conduct #S transaction on a monthly basis to ensure Appendix D – User ID's document corresponds.

10.7.8 That each current user has signed the Appendix A – Proper Use Declaration

10.7.9 That the audit transaction log is continuous and no pages/entries are missing.

10.8 The above Security Programme Manager conducting the audit should then select a minimum of 5% of the entries on the print out, for each selection it should be checked that:

10.8.1 There is an approved form for each check made.

10.8.2 The form POL208 and any other agreed forms meet the criteria as listed in section 9 of this document.

10.8.3 The information entered on to the PNC to make the check matches that of the request form.

10.8.4 The correct result has been entered on the form for example, 'PNC no trace / No relevant information / PNC print returned to requestor' and that it has been initialled by the PNC operator who carried out the check

10.9 The result of the audit should be detailed on the Audit Report.

10.10 Audit reports and the #TE prints should be kept for a minimum of 15 months.

10.11 The above Security Programme Manager conducting the audit should initial the audit acknowledgement of findings and any 'Corrective Action' requirements. These should be discussed with the relevant Senior Security Manager if appropriate.

10.12 The Security Programme Manager responsible for PNC will be responsible for any actions required by the audit report, including establishing the reasons behind any 'missing' forms.

10.13 If any inappropriate use of the PNC has been discovered, an Appendix F / PNC3 form must be completed. The Security Programme Manager is responsible for ensuring that the Senior Security Manager is informed as soon as is reasonably practicable.

10.14 Post Office Ltd Security will conduct a self-audit of the entire process on a yearly basis to ensure that processes and procedures are adhered to.

11. Incident Management

All breaches of this policy and security incidents must be managed appropriately. All breaches will be notified to ACPO via the NPIA.

A breach of policy is defined as any action that contravenes the spirit or word of this document. A security incident is where actual misuse or compromise of the PNC or its data has occurred. A breach of policy may or may not lead to a security incident. For example, leaving the PNC terminal logged on and unattended is a breach of policy but it may not result in an incident. If the terminal left unattended is used by an unauthorised person, then an incident has occurred. In this example, if only the breach of policy has occurred, it can be handled entirely in-house. If the incident had occurred, it must be notified to the NPIA.

The following types of incident must be notified to the NPIA without delay:

- any unauthorised Names check;
- any unauthorised Vehicle check;
- any unauthorised disclosure of PNC data – accidental or malicious;
- any unauthorised modification or deletion of a PNC record;
- any instance of using the PNC for an unauthorised purpose;
- any other misuse of the PNC, which could result in harm or embarrassment to an individual or which could lead to adverse publicity for the organisations involved.

All breaches will be reported to the Head of Security via the Senior Security Manager to determine appropriate disciplinary actions.

In line with the above, breaches and incidents should be notified to the NPIA Information Assurance Manager, who will assist the investigation if required. You must keep the NPIA Information Assurance Manager up-to-date with the investigation and submit a full report at its conclusion.

Appendix A – Proper Use Declaration

The PNC Security Operations Manual requires all staff and contractors, who access the PNC, to sign a statement regarding making proper use of the system and its data.

I, ..., understand and accept that, in order to log onto the PNC, I must be an authorised user, be in possession of a PNC User ID that is unique to me and have a reason governed by my current job function. I also understand and accept that I may only access or attempt to access those PNC transactions to which I have been authorised, use the transactions for a legitimate, business/policing purpose and use any knowledge obtained for authorised business/policing purposes only.

I have read and agree to abide by the Post Office Ltd PNC Security Operating Procedures.

Signed .... Date ....

Appendix B – POL208 Form

Please click on icon for the POL208 PNC request. It is noted this form is also used for a number of other Security Manager requests.

POL208 v1.3

POL00105229

Appendix D – User ID's

The PNC Appointment Document requires details of all staff and contractors, who access the PNC, along with their User Name, User ID, Date of change/addition and signature of appropriate senior officer for PNC usage.

User Name	User ID	Date of Change / Addition	Details of Change / Addition	Authorising Signature

POL00105229

Appendix E – Password Reset

The PNC Password Reset requires details of all staff and contractors, who access the PNC, along with their User Name, User ID, who require password reset

User Name	User ID	Date of Password Reset	Details of Password Rest	Authorising Signature

Appendix F / PNC 3 - Breach/Suspected/Attempted Breach Of PNC Security

IMMEDIATE TIME: DATE:

1. Do you know the identity of the person? If so, who was it? If not please describe them.

2. What did they do?

3. What information did they get, if any?

4. Was an Operator's ID or password used? Which one, if known?

5. Who else saw the incident?

6. Informed the Security Programme Manager at time: date:

Signed:

A) Form seen & appropriate action taken:

B) Action by :

C) NPIA informed: time: date:

Appendix G /PNC 5 - Persons Registered to Use/Operate the PNC Terminal

Updated 29 Aug 2012

Name	Date Commence d	Date Ceased	Browser Training Date	Vehicle Enquiry Training Date	VODs Training Date	User Group
Mark Dinsdale	18 July 2012		26 April 2012	n/a	n/a	VSPAR354
Amy Hutton	18 July 2012		25,26 & 27 April 2012	25,26 & 27 April 2012	17 July 2012	VSPAR354
Jayne Bradbury	18 July 2012		25,26 & 27 April 2012	25,26 & 27 April 2012	17 July 2012	VSPAR354
Fazila Sheikh	18 July 2012		25,26 & 27 April 2012	25,26 & 27 April 2012	17 July 2012	VSPAR354
Girish Patel	18 July 2012		25,26 & 27 April 2012	25,26 & 27 April 2012	17 July 2012	VSPAR354

Appendix H / PNC1 – Log On Sheet

DATE	NAME	SIGN ON	SIGN OFF	SIGNATURE	START NO	FINISH NO

POL00105229

Appendix I ‘PNC Requests Authorising Managers Instruction Policy’.

All PNC Requests Authorising Managers must on an annual basis read and abide by the PNC policy to ensure all requests are requested in accordance with the PNC Security Operations Manual.

PNC Authorising Managers Instruction