Police National Database (PND) Procedure

This document is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement

The Police National Database (PND) is a national data store of operational policing information and intelligence provided by individual forces. It is not an evidential system. It contains copies of locally held police records covering intelligence, crime, custody, child protection and domestic abuse investigations. Details of record types shared by each force/agency is available within the PND and on the North Yorkshire Police (NYP) PND Bulletin Board.

The PND is updated frequently allowing users to search for information and intelligence relating to people, objects, organisations, locations, and events. It identifies associations between PND records and enables the viewing of flags, warnings, and alerts.

The statutory PND Code of Practice came into effect on 31 March 2010. It sets out a framework for the use of the PND and information obtained from it. Chief Officers of England and Wales must have regard to the Code when determining PND policies and procedure.

The PND Manual of Guidance and Business Rules sets out strategic and tactical guidelines for consideration by Chief Officers when developing PND policies and procedures. The Manual provides guidance to all police staff and PND users. It is particularly intended for police managers, directors of intelligence, senior investigating officers, and heads of those departments in which PND is used.

NYP will operate the PND in accordance with the Code of Practice and the Manual of Guidance and Business Rules.

Procedures:
Protective Marking Procedure
Review, Retention and Disposal of Information Procedure
PND Access Control Procedure

Other Documents:
Information Management APP - Management of Police Information

Current PND guidance and reference documents are available within the library of the Police National Database group on the Knowledge Hub. These documents are available to PND users and non-users alike.

Process

1. Governance

1.1 The Head of Criminal Justice has overall authority of the PND at NYP. The Force Intelligence Bureau (FIB) Detective Sergeant (DS) is the lead Force Single Point of Contact (SPOC) and the PNC & PND Manager is the PND Registrar.

1.2 The NYP PND User Group (chaired by the PNC & PND Manager and attended by key business areas: Access Control roles, Auditing roles, Operational roles) is established to discuss PND policy, procedure, and processes, and ensure PND usage by NYP is maximised.

1.3 The PNC & PND Manager represents NYP at the Regional PND User Group.

2. NYP Requirements to Access PND

To access PND North Yorkshire Police must:

- Have in place a Risk Management and Accreditation Document Set approved by the National Accreditor (Home Office)
- Implement a robust audit regime
- Upload data daily, where possible, to the PND
- Maintain a contract, via the National Home Office Framework, to receive the Home Office Identity Access Management (IAM) services. IAM controls access to national and local IT systems, including PND.
- Renew the IAM Device Certificate yearly.

3. Available Data Types

3.1. The PND can be viewed in either a Confidential environment or Restricted environment. The majority of PND Users will access PND in the restricted environment (PND Restricted), and a smaller number of PND Users will require access to PND in the confidential environment (PND Confidential). Roles which require PND Restricted or PND Confidential have been identified by the PND SPOC/ Registrar.

3.2. In an Information Sharing Declaration to the Home Office, NYP has stated that the following data will be shared and updated daily where possible

- Niche and Indepol crime – all crime occurrences that have a validated Home Office returnable stats classification excluding Fraud, any suspects, or offenders (person or organisation), occurrence addresses, property link to these occurrences with the classifications indicating Stolen, Damaged, Lost, Recovered, Safekeeping or Used in (excluding Investigation Property, Police Documentation and Vehicle licences) and Offences associated to the crime

- Niche and Admin of Justice custody – all occurrences that have an arrest record attached, the detainee, along with the risk assessment, what the arrested was for, offences charged with and Police and Criminal Evidence (PACE) Act 1984 bail and the location at which the arrest took place
- Niche and Case Administration Tracking Systems (CATS) child abuse - All child abuse occurrences (criminal and non-criminal), any suspects, offenders, subjects, main nominals or victims and occurrence addresses
- Niche and Indepol domestic abuse – All domestic occurrences (criminal and non-criminal), any suspects, offenders or victims and occurrence addresses
- Niche and Indepol intelligence – All information linked to a handling code one, two, three and four occurrences will be shared unless the intelligence carries the status of 'Processing in progress' or 'Reviewed no value'. There will be a flag to indicate to Forces that NYP holds information that is graded as handling codes five. Any subjects of Intelligence (Person or Organisation) and occurrence addresses will be shared
- Victim information associated to any Schedule 3 or 5 offences under the Sexual Offences Act 2003, and victim information in child protection and domestic not subject to the previously mentioned Schedule 3/5 offences. The information sent on victims is the same as any other nominal, no person fields are removed or added
- Management of Police Information (MoPI) grading against the nominal and their review date (when this data becomes available)

3.3 Witness information will not be uploaded to PND

3.4 PND data quality and the mapping of Niche codes to PND will be overseen by the PND Registrar (PNC & PND Manager).

4. Access

4.1. PND is implemented in the following locations with Confidential or Restricted access designated by the PND Registrar.

4.2. Access Control Roles (Confidential Access):

- PNC
- ICT

4.3. Data Upload Roles (Confidential Access):

- ICT

4.4. Auditing Roles (Confidential Access):

- Information Management
- Professional Standards & Integrity Unit (PSIU)
- Inspection & Strategic Planning

4.5. Operational Roles (Restricted Access or Confidential Access):

- Civil Disclosure

- CID
- Firearms Licensing
- Information Management
- Intelligence
- Initial Enquiry Team
- Major Crime Unit
- MAPPA
- Organised Crime Unit
- Operational Support Unit
- PNC Liaison & Records
- Professional Standards Integrity Unit (PSIU)
- Safeguarding Hub
- Special Branch
- Vetting

4.6. PND Single Point of Contact (SPOC) for external request :

- Force Intelligence Bureau (FIB) Detective Sergeant (DS)

4.7 A guide titled 'Use of PND in your Role' sets out some examples of how the PND could assist users from different business functions

5. User Requirements for Access

5.1. Prior to gaining access to PND all users are required to:

- Complete the process detailed in the PND Access Control Procedure
- Complete the pre-course material, as detailed in the pre-course PND Joining Instructions, prior to attendance at the PND training course
- Complete the PND training course
- Agree to attend mandatory refresher training every 2 years and made mandatory for attendance to maintain competency
- Sign and submit the End Entity Agreement (Confidential users only)

5.2. IAM logon credentials (username and password) will be issued to the user on successful completion of a PND training course. PND Confidential users will also receive a smart card with PIN.

5.3. Should any PND user be found not to be utilising the system for a period of three months, then a warning will be sent to the user and line manager. If inadequate use is still evident after a further 30 days, then PND access will be removed by the PNC & PND Manager or delegate. Should it be deemed that the user does need PND access they will need to attend a further course as directed by PNC Liaison and Learning and Development, however attendance would need to be justified and supported by the users first and second line managers.

6. Rules for Using PND

6.1. Recording PND Enquiries for Audit Purposes

- All PND searches require justification to support the transactional audit process outlined in section 9 of this procedure.
- The requesting officer/staff member will record the details of the request and the reasons for the search in an Occurrence Enquiry Log (OEL) update on Niche.
- The PND User will record the justification and the identity of the requesting officer/ staff member in the relevant field(s) of the PND.
- The PND User will ensure that the appropriate justifications/reasons for carrying out a PND enquiry are correctly recorded in PND, in order that meaningful management information can be produced from it. The justification/reason of 'Other' should not be routinely used.

6.2. Handling of PND data (storage/retention/disposal)

- PND data can be extract or printed, if PND has been accessed via the Restricted platform, using the functionality outlined in the PND Search User Guide.pdf
- The protective marking provided by PND, must be adhered for the extraction, printing, storage, disposal, handling and retention of PND data to prevent unauthorised access to, theft or loss of data. Refer to the NYP Protective Marking Procedure and Review, Retention and Disposal of Information Procedure for further information.
- All PND extracts or print data will include the Protective Marking, watermarks, data protection warnings, justification for print, who produced the print, and on whose behalf, as prompted by the PND. The copy and paste function must not be used.
- This process will ensure NYP is able to maintain an audit trail of PND data.

7. Use Of PND

7.1. PND can be used for authorised PND Checks

- PND enquiries are authorised for any policing purpose and PND Users are reminded of their obligation to use their PND training, and access PND in their daily tasks. A PND enquiry can be carried out by a PND User in relation to their daily duty or as part of a specific tasking. PND Users are authorised to conduct enquiries on behalf of other NYP police officers/staff, in addition to their own duties. Any enquiry must only be conducted for a lawful purpose and will be subject to audit.

7.2. Local PND Enquiries

- Images obtained during an investigation or other police activity of a suspect, victim or witness who is yet to be identified, PND User will assess the quality of the image and ensure it is appropriate to be used for Facial Search within PND. If the image can be used and the search is in line with 7.1 a search will be undertaken. PND does not provide confirmation that a probe image exactly matches an image in PND, it provides images that are similar therefore providing potential lines of further enquiry.
- Where a request (of any type) is made to a PND User by an NYP officer/staff member, the result of any such enquiry can be passed to the requesting officer/ staff member. The method of passing the information will be done in accordance with the relevant protective marking of the originating Force/Agency as provided in PND.

7.3. PND Records as Evidence

- PND records must not be used as evidence. Where information gained from PND is required in evidential format, the originating force/agency must be contacted to provide this. PND records must not be used to form part of the unused material in a court case, without the knowledge and consent of the originating force/agency.

7.4. Sharing of Information

- Where PND data is to be shared outside the Police Service, it must be done in accordance with an established Information Sharing Agreement (ISA), Memorandum of Understanding (MOU) or via a specific legal gateway. Where any doubt exists, the officer/ staff member should consult their line manager or Civil Disclosure.

7.5. Requesting Further Information from Another Force

- PND Users, through the originating Forces' PND SPOC:
    - Can request further information
    - Must request to use PND information in evidential process

7.6. Response to Requests for Additional Information

There are nationally agreed response times set out in the Investigatory Powers Act 2016, the Investigatory Powers Act 2000 & Interception of Communications Codes of Practice, which is already in use by law enforcement agencies (LEAs). On a PND request, users will need to indicate the priority code. These codes follow those set out by the standards:

- Priority code one:
    - Preventing an immediate threat to human life in an emergency
- Priority code two:
    - Where arrests planned and imminent (within the next 24 hours) for serious crime are taking place, or prisoners are in custody and the data is required to secure a charge where bailing the suspect is not in the public interest, or
    - Where it is known that the data is required to prevent the immediate disposal of evidence connected to serious crime (within the next 24 hours), or
    - To prevent serious injury to any person (within the next 24 hours) where there is a direct threat, or when it is necessary to risk assess the deployment of law enforcement officers (in the next 24 hours) during an operation and the risks cannot be assessed by any other means or
    - The enquiry relates to a child or other vulnerable person
- Priority code three:
    - In response to any enquiry involving any death which commenced within the last 14 days

- Priority code four:
    - In connection with an investigation of serious crime, or where effective Court dates has been set for either a Committal, Plea and Direction Hearing or trial
- Priority code five:
    - All other enquiries

Within the PND request, the user will also indicate timescales for response using the following:

Reply Urgent	2hrs
ASAP	24hrs
Routine	3 days
Specific Date	dd/mm/yyyy
Non-urgent	7 days

Timescales have not been directly associated with a particular priority code as there will be exceptions e.g., a priority code four could attract any response time between urgent and non-urgent, dependent upon whether a trial has been adjourned for that response, or if the trial has not yet started. The originating Force's PND SPOC will agree response times with the requesting Force.

7.7. Refusal to Respond

The originating Force's PND SPOC has the right to refuse to respond to an external PND request for information on the following grounds:

- The request is deemed to be unreasonable due to the nature of the enquiry or the volume of records requested
- The enquiry is not deemed to be for a policing purpose
- The request is not clear or focused
- The information requested is of a sensitive nature and the Force takes the decision not to disclose
- The PND SPOC will explain their reason for refusal in their response to the user.

8. Single Point of Contact (SPOC) Arrangements

8.1. The NYP PND SPOC function within the FIB is to act as the gatekeeper for all external Forces' PND related enquiries. This includes receiving any requests for additional information not available in the PND.

8.2. Any requests in relation to the further dissemination of intelligence with a handling code four or five are to be handled through the FIB.

9. Audits

9.1. The PND has advanced audit capability in relation to any action or enquiry carried out in the PND. Any data extracted from the PND and stored in a local information source, will be subject to local management and storage arrangements.

9.2. An audit will be completed for every PND User at least once within a 6-month period.

9.3. As part of the audit, PND Users will be contacted by the PND Auditor, to provide appropriate justification for the PND transaction. First line managers of the PND User will be asked to verify the information provided and confirm that that the transaction has been completed for a policing purpose.

9.4. An audit log will be maintained to ensure the integrity of the transactional data and therefore guard against the improper use of PND.

9.5. Monthly Schedule for Standard Search Audits:

- 1% dip sample of all PND Standard Searches

Trained PND Auditors from the Inspection and Strategic Planning Team will conduct the PND Standard Search audits and maintain a log of the audits undertaken and the responses received.

9.6. Monthly Audit Schedule for Non-Standard Searches

- At least 3 transactions or 5% of all transactions (whichever is higher) of all PND Non-Standard Searches
- Trained PSIU staff will conduct the PND Non-Standard Search audits and maintain a log of the audits undertaken and the responses received from line managers

RESPONSIBILITIES

The following is a list of the responsibilities of individuals to comply with the application and monitoring of this procedure.

Operational Officers/Police Staff

Access Control Roles: As detailed in the PND Access Control Procedure

-
- PNC & PND Manager, PNC & PND Coordinator, PNC & PND Support Officer
- Head of Professional Standards Department (PSD) (no access to PND, but part of Access process)
- ICT (no access to PND, but part of Access process)

Daily Data Upload Roles:

- ICT

RMADS compliance:

- ICT
- Information Management

Auditing Roles:

- Inspection & Strategic Planning: PND Standard Search Auditors

- Professional Standards & Integrity Unit (PSIU): PND Non-Standard Search Auditors

IAM Contract Renewal & IAM Device Certificate Renewal

- Regional Procurement (IAM contract)
- ICT Infrastructure Support Engineer (IAM Device Certificate Renewal)
- PND Registrar (Approval of IAM Device Certificate Renewal)

Operational Roles: PND Users

- Civil Disclosure
- CID
- Firearms Licensing
- Information Management
- Intelligence
- Initial Enquiry Team
- Major Crime Unit
- MAPPA
- Organised Crime Unit
- Operational Support Unit
- PNC Liaison & Records
- Professional Standards Integrity Unit (PSIU)
- Safeguarding Hub
- Special Branch
- Vetting

PND Single Point of Contact (SPOC):

- Gatekeeper for external force PND enquiries

PND Registrar:

- Owner and maintenance of PND Register
- PND Data Quality (oversee mapping of Niche codes to PND Data)
- Chair PND User Group
- Attend Regional PND User Group
- Manage PND training nominations lists
- Prioritise nominated staff for PND training courses

Training Services:

- Provision of PND Training

First Line Supervision of PND Users

- Responding to PND Auditor requests
- PND Access Control

Safer Neighbourhood Commanders/Heads of Department

Head of Criminal Justice

- Lead and Owner of PND

Head of ICT

- Certificate renewal (IAM); PND Access compliance (RMADs and Daily data uploads)

Command Team

- Assistant Chief Constable

Definition of Special Terms

PND – Police National Database
IAM – Identity and Access Management