**Police National Computer (PNC) Procedure**

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

## Statement

The PNC lead for NYP is ACC Mark Pannone.

The PNC provides quick and direct access to a central store of information. The information is accessible by police and law enforcement agencies throughout England, Scotland, Wales, the Channel Islands, and the Isle of Man, together with a range of other authorised agencies. It contains information relevant to the following:

- Vehicles registered at DVLA
- Unregistered and foreign vehicles of police interest
- Stolen and found property
- Individuals processed for criminal matters
- Individuals otherwise of police interest (e.g. missing or subject to court order).

Other agencies providing information relevant to the above include:

- Her Majesty's Courts
- Her Majesty's Prisons
- Driver and Vehicle Licensing Agency (DVLA)
- Motor Insurers Bureau (MIB)

NYP will utilise PNC data to ensure safer roads, efficient delivery of justice and the reduction of crime and disorder in our communities. To maximise the benefits of PNC we will:

- collect and update the PNC with good quality, accurate & relevant data
- Use PNC data as an effective contribution to operational policing and decision making
- Maintain an adequate pool of staff skilled in analysing, creating, and retrieving PNC data 24 hours a day, 7 days a week

Our ability to police effectively and deliver criminal Justice efficiently relies upon accurate and timely PNC information. In handling PNC data, NYP will observe the PNC Code of Practice, the PNC Manual and recommendations contained within the HMIC thematic inspection 'On the Record'.

**Overarching Policies:**
Information Security Policy
Data Protection Policy

**Procedures:**
Deletion of Records from National Police Systems Procedure

**Other Documents:**
NPCC Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1)
Deletion of Records Application
HMIC On the Record
PNC Code of Practice 2005
National PNC Manual

**Process**

**Governance**

Use of the PNC is governed by the Data Protection Act 2018 and Computer Misuse Act 1990.
The National PNC Manual defines operating standards to which all PNC users must adhere.
The PNC Code of Practice 2005 enshrines the principles of effective and legal use of the PNC.
All NYP staff will guard against unlawful use or disclosure of PNC data.

**Security**

PNC data is classified as OFFICIAL and must be handled as such.

Should any member of staff receive a request for a PNC check where they suspect the enquirer may not be who they claim to be they will not carry out a PNC check but will:

- Obtain contact details and details of the information sought by the enquirer
- Advise the enquirer they will call back.
- Pass all information to a line manager who will attempt to verify the enquirer's identity.

PNC Liaison must be informed at the earliest opportunity where enquiries establish the enquirer has provided false credentials to gain access to PNC information. PNC Liaison will use the PNC broadcast function to alert PNC Services and other police forces to the bogus request.

**Access and Disclosure**

Access to PNC data is permitted for a legitimate policing purpose or to fulfil a common law duty. The reason for every check should be clearly recorded within the PNC log line.

The handling of personal and sensitive personal information is subject to legislative requirements under the Data Protection Act and General Data Protection Regulations. Wilful failure to observe

relevant legislation and guidance may result in disciplinary procedures or legal action for which a period of imprisonment can be imposed.

Various teams within NYP are responsible for disclosing PNC information in line with their duties. These include, but are not limited to the following:

- The Force Control Room disclose limited information to authorised persons from non-police organisations to fulfil agreed purposes. A list of authorised persons is maintained and allows the verification of enquirer identity. PNC information will only be disclosed to authorised persons and a record of each enquiry maintained.
- The PNC Bureau, PNC Records Office and Prosecution Team may disclose PNC information to non-police prosecuting agencies to support their investigations, decision making and prosecutions. Except where a separate agreement exists, such disclosures will comply with the NPPA National Standard.
- Other NYP departments are permitted to share information where disclosure is supported by an Information Sharing Agreement (ISA) or legislation.

Hard copy disclosure to external organisations will be by way of the appropriate PNC print. All PNC prints must be handled in accordance with the appropriate protective marking (Official). PNC prints may be sent by email but only where the recipient has access to a secure email address.

**PNC Enquiry**

Manual PNC checks may be carried out on desktop machines or mobile devices. Staff must complete accredited PNC training before being provided with a role-based PNC account. Each user will be provided with a user ID and password and will be required to change that password immediately upon logging in for the first time. All PNC user accounts are for use by the person to whom the credentials have been provided. Individual user credentials must not be shared with any other person.

Prior to carrying out a PNC check on behalf of another the PNC operator must satisfy themselves:

- Of the enquirer's identity and entitlement to receive the requested information; and
- The PNC check is being requested for a permitted purpose; and
- Access to the PNC complies with published guidance including the National PNC Manual

**PNC Update**

NYP will update the PNC with accurate and relevant Information in a timely manner. Timeliness of PNC updates shall be compromised only where necessary to confirm accuracy and ensure compliance with legal and procedural requirements. Appropriate supporting information will be maintained and retrievable promptly day or night.

Staff carrying out PNC updates will have completed accredited PNC update training and be required to maintain proficiency in those skills.

PNC Bureau and PNC Records Office team leaders will conduct regular quality assurance checks on updates performed by their teams. Up to 100% of updates may be subject to quality checking based upon risk and operator capability.

**Auditing**

Every PNC user is responsible for keeping an accurate record of PNC transactions through good use of the PNC log line. The log line should reflect the enquirer and the reason for the check or, where the check is for operational purposes (e.g. a stop/check), a full location. Where possible, a unique reference number and brief incident description should be included. Details of the enquirer will be recorded at the start of the log line in 4-digit format to allow differentiation from other numerical information and aid future searches. Vehicle call signs will not be used.

PNC Liaison will conduct periodic checks to review volume of usage, quality of log line data and compliance with other national guidance regarding access to third party data via the PNC. Access may be withdrawn where inappropriate or insufficient use is identified.

Inappropriate use may consist of access to data contrary to this or any other NYP procedure, other published guidance, or legislation. Failure to enter sufficient PNC log line information in accordance with requirements over a sustained period and following guidance may also constitute inappropriate use.

Where the volume of checks completed by a PNC user falls below the minimum standard this may result in withdrawal of access on the grounds of insufficient use. The National PNC User Manual requires withdrawal of PNC access where the user has not performed a check in an area of PNC within the previous 6 months. PNC access may be reinstated in the circumstances set out below:

- Last PNC check within 12 months – complete nationally agreed assessment for the areas of PNC they need to access.
- Last PNC check within 12-24 months – complete refresher training for the areas of PNC they need to access.
- Last PNC check more than 24 months ago – required to attend PNC training in the PNC area to which access required.

PNC Liaison may exercise discretion when considering whether to remove PNC access or reinstate without requiring the user to complete a PNC Assessment. When using discretion PNC Liaison will consider PNC usage in the preceding 12 months and particularly:

- Volume of checks; and
- Quality of log line information; and
- Compliance with legislation, national guidance, and local procedure.

**PNC Retention Policy**

In accordance with the current PNC retention policy, all PNC offence processing information will be retained until the data subject reaches 100 years of age. Requests for the early deletion of PNC information and associated biometric data (fingerprints/DNA/custody image) may be made in certain circumstances. Further information is available on the ACRO Deletion of Records from National Police Systems webpage.

**<u>Responsibilities</u>**

**All Operational Officers/Police Staff**

Ensure any request for PNC update is accurate, relevant, complete and timely.
Respond promptly to requests for clarity to ensure PNC updates are not unnecessarily delayed.

**PNC Operators**

Comply with PNC guidance and best practice conveyed during training and on the PNC Source site.
Access PNC only for legitimate purposes and disclose only to those authorised to receive PNC data.

**PNC Liaison**

Ensure NYP PNC use complies with legislation, national guidance and published best practice.
Maintain a record of authorised PNC staff and manage user permissions and groups appropriately.
Provide advice and assistance in respect of specialist PNC enquiries.
Assess and respond to applications for the deletion of data from national police systems.

**PNC Records**

Carry out PNC updates and quality control checks as they relate to offence processing ensuring updates achieve statutory timeliness targets where possible.

**PNC Bureau**

Carry out a wide range of operational PNC updates and searches against vehicles, property and nominal records ensuring updates are prompt and without unnecessary delay.

**Force Control Room**

Maintain a list of staff from non-police agencies who are authorised to request PNC information.
Ensure the list contains sufficient information to allow for the verification of enquirer identity.

**Learning & Development**

Ensure PNC training is delivered to defined standards by PNC accredited trainers.
Inform PNC Liaison upon completion of every PNC course or assessment to allow for appropriate updates to PNC user permissions.

**Human Resources**

Inform PNC Liaison of new starters, temporary and permanent role changes, secondments, and leavers to allow for appropriate updates to PNC user permissions