
SI Identification Number	SI0319
---------------------------------	--------

Policy Ownership	Innovation and Standards Department
-------------------------	-------------------------------------

Issue Date	01/08/2019
-------------------	------------

Review Date	5 years from issue date
--------------------	-------------------------

Governing Service Policy	Criminal Justice
---------------------------------	------------------

Cancellation of	SP01/2015 The Police National Database
------------------------	---

Classification	OFFICIAL [PUBLIC]
-----------------------	--------------------------

SI0319

National Enquiries

This Service Instruction gives guidance in relation to conducting enquiries throughout the United Kingdom.



Table of Contents

1. Introduction	3
2. The Police National Database (PND)	3
3. Gazette	6
4. Police National Computer (PNC)	6
5. PNC Updates	6
Appendix A Contact Us.....	8

1. Introduction

The National Enquiries Unit has responsibility for the following business areas within The Police Service of Northern Ireland (PSNI):

- Police National Database (PND) Single Point of Contact (SPOC);
- Gazette Function; and
- Police National Computer (PNC) SPOC.

2. The Police National Database (PND)

The Police National Database (PND) was established directly as a result of recommendations made within the [Richard Inquiry Report](#) in 2004.

The PND is a National repository for UK Police information including intelligence.

The PND enables the PSNI and a number of other law enforcement agencies to share, access and search locally held information on a national basis, overcoming artificial geographical and jurisdictional boundaries.

Where an officer becomes aware that any part of their investigation has a national aspect, the appropriate enquiry should be

forwarded as soon as possible to a PND user.

Local systems and the Police National Computer (PNC) must be checked before a PND search is conducted.

PND does not replace the PNC check. PNC remains the principal database by which a person is checked against the criminal records index; wanted or missing persons are circulated; stolen or found property is recorded; and other criminal record information is stored.

PND on the other hand provides access to police information and intelligence. Both PNC and PND should be checked in relevant situations, for example: a vehicle's registered keeper is available from PNC whilst intelligence on the vehicle and the keeper can be obtained from PND.

Non PND users with non-urgent inquiries can request a PND check by completing a "PND Search – PND Single Point of Contact" form and sending it via e-mail to a relevant PND user / PND SPOC.

Urgent requests should be made directly by phone or in person to a PND user / PND SPOC or PVI. Subject to validation a PND check will be carried out. The requestor **must** then complete a follow up PND search request form as soon as practical.

All request forms from PSNI PND Users to other UK forces must be submitted via the PND SPOC Office. It is the responsibility of the user to ensure this form is submitted.

If an urgent request is made in person and the requestor is not known to the user, the requestor must:

- Produce a valid identity card along with service/staff number for the check to proceed.

If an urgent request is made by phone, and the requestor is not known (identifiable by their voice) to the user, the user must:

- Call back the requestor on a mobile phone recorded against that person on the PSNI's intranet.

It will not be deemed acceptable to call the requestor back on an internal extension number, although that shows the requestor to be using a PSNI phone, it does not establish the true identity of the requestor.

The PND SPOC Office, Innovation and Standards Department acts as liaison between the PSNI and other UK forces with all incoming and outgoing requests for information following a trace result on PND.

All external requests for PSNI intelligence will be managed by the PND SPOC **only**

after consultation with C3 Service Intelligence Bureau (SIB).

On receipt of an external request, the PND SPOC will record details for audit purposes. If the SPOC can resolve the enquiry directly they will do so. If further internal enquiries need to be made then the SPOC will contact the relevant department/branch.

For requests for further information from other forces, a request form **must** be completed and submitted to the PSNI PND SPOC Office where records will be maintained for audit. PSNI PND Users should not request information directly with another force's PND SPOC.

The dissemination of information from PND must (in all but exceptional circumstances) be carried out in accordance with the Government Security Classification Policy (GSC).

PND search results may be disseminated only for a policing purpose. If a PSNI PND user has conducted a search and found relevant CONFIDENTIAL material which needs to be disseminated to the requestor, in non-urgent cases this should normally be disseminated by internal e-mail, in **urgent** cases this may be disseminated by phone but a written record should be kept locally

of verbal results given. Before dissemination of PSNI intelligence, SIB should be consulted and their Intelligence Officer will be the decision maker as to whether this intelligence should be shared.

If in **urgent** circumstances, the risks around the delay of sharing the information are deemed to outweigh the risks of breaching the GSC handling instructions, then a user can disseminate PND data in a manner outside that guidance. However, the user must use the most secure means of dissemination available in the particular circumstances.

Where a user has to breach GSC guidelines in disseminating information, they should record the breach and the justification for it.

Despite the provision above, the importance of taking information security seriously in respect of PND data cannot be over-emphasised.

- Use of the system is dependent on having the **trust and confidence** of other UK forces and any unreasonable breaches of information security procedures will only help to erode that trust and confidence and undermine the effective use of the PND.

- Officers and Staff who breach GSC requirements without good reason will find their access to the system withdrawn and may be subject to misconduct proceedings.

PSNI Officers and Staff, who in the course of their duties work with partner agencies, may share PND data with those partners in accordance with the extant Service Level Agreements (SLA) and Memorandum of Understanding (MOU) were:

- There is a statutory power or information sharing protocol in place but users must be mindful that disclosure is consistent with the individual's rights of privacy under Art 8 of the European Convention of Human Rights; and
- Any requirement to share PSNI intelligence **MUST** be managed by SIB, C3 HQ.

Permission must be sought from the relevant force when PND information is required for court or disclosure purposes. All requests must be submitted via the PND SPOC office.

3. Gazette

The Gazette team are responsible for the circulation and cancellation of Wanted/ Missing Persons on PNC.

For information:

- A written authorisation is required from an Inspector (or above) before a 'Wanted' flag can be added to PNC.
- A 'Locate and Trace' flag does not require written authorisation
- The PNC flag must be cancelled at the time the NICHE flag is cancelled.

Please refer to PSNI guidance on Police Action in respect of Missing Persons.

4. Police National Computer (PNC)

The strategic aim of the Police National Computer (PNC) is to provide the best possible information for operational policing purposes.

Police Officers and Staff can use PNC to carry out enquiries in relation to persons, property and vehicles.

The PNC provides details on the following:

- An offender's criminal record;

- Modus Operandi (way of operating);
- Associates;
- Aliases; and
- Distinguishing features.

The PNC names application also holds information on whether offender is:

- Disqualified from driving;
- Subject to a Sexual Offender Registration; or
- Subject to a European Arrest Warrant.

5. PNC Updates

The PNC Updates team are the Single Point of Contact (SPOC) for PSNI PNC queries.

The SPOC team are responsible for both internal and external requests.

Externally, any enquiry resulting from a PNC search by a UK force can be dealt with by the SPOC team. This covers a range of areas such as:

- Real time information exchange on persons stopped or sought;
- Further information on Flags or Warnings;

- Further information on convictions or person details held on local systems; and
- Updates to PNC or Northern Ireland Criminal Record Viewer (CRV);

Where necessary the SPOC team will refer the requestor to another department or put them in direct contact with the officer.

Internally, any enquiry resulting from a PNC search by a PSNI officer can be dealt with by the SPOC team. This covers a range of areas such as:

- Dual amendments to existing PNC and CRV records in line with national agreements;
- PNC data quality projects;
- Management of PNC record merging;
- PNC conviction information required for evidence in court; and
- Other updates to person record including flagging or deceased.

Should any officer require a PNC print when carrying out their investigation they should contact the SPOC team.

Appendix A Contact Us

Service Instruction Author

National Initiatives

Branch Email

zPNDSPoC@psni.pnn.police.uk

zGazetteSection@psni.pnn.police.uk

zPNCUpdates@psni.pnn.police.uk