Ministry of Justice

HM Prison & Probation Service

Policy name: Use of the Police National Computer in prisons

Publication Date: 06 June 2023 **Implementation date:** 06 June 2023

Replaces the following documents which are hereby cancelled: PSO 0905: Operation of the Police National Computer

Introduces amendments to the following documents: None

Action required by:

X	HMPPS HQ	X	Governors
X	Public Sector Prisons	X	Heads of Group
X	Contracted Prisons		The Probation Service
	Under 18 Young Offender Institutions		Other providers of Probation and Community Services
	HMPPS Rehabilitation Contract Services Team		

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information: By the implementation date Governors[1] of Public Sector Prisons and Contracted Prisons must ensure that their local procedures do not contain the following: *PSO 0905*

Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

Section 6 of the Policy Framework contains guidance to implement the mandatory requirements set out in section 4 of this Policy Framework. Whilst it will not be mandatory to follow what is set out in this guidance, clear reasons to depart from the guidance should be documented locally. Any questions concerning departure from the guidance may be sent to the contact details below.

References to staff and employees of HMPPS shall be taken to mean any such person engaged in HMPPS work using PNC, including non-directly employed persons.

How will this Policy Framework be audited or monitored: Under arrangements to be put in place by the Governor according to guidance issued by the police and under this framework.

Resource Impact: This framework updates and re-implements PSO 0905 as a policy framework without any change to the resourcing requirements.

Contact: pncenquiries@justice.gov.uk

[1] In this document the term Governor also applies to Directors of Contracted Prisons.

Deputy/Group Director sign-off: Andy Rogers, Deputy Director, Operational Security Group

Approved by OPS for publication: Sarah Coccia (Executive Director Prisons), Chair of Operational Policy Sub-Board, May 2023

CONTENTS

1. Purpose and definition

1.1 The Police National Computer (PNC) is a system that stores and shares criminal records information across the UK. The service is provided by the Association of Chief Police Officers Criminal Records Office (ACRO). Law enforcement agencies use it to access information that will support national, regional and local investigations. PNC services are provided to support the criminal justice work of a range of organisations including HMPPS.

1.2 The purpose of this framework is to set out the requirements for provision of access to PNC equipment and information for those prisons and individuals in HMPPS (including non-directly employed persons undertaking any work on behalf of HMPPS) authorised by the police to use it;

1.3 To prevent unauthorised access to PNC equipment and information;

1.4 To set out the responsibilities and obligations of Governors of prisons with access to PNC equipment, and to ensure that such responsibilities and obligations are met.

2. Evidence

2.1 There are currently 43 prisons (the number may change from time to time) with PNC equipment installed in prisons with others being considered. These prisons have designated operators who are appointed to use PNC equipment as required and have been trained and been checked at the appropriate level of security vetting clearance to do so.

2.2 Other HMPPS staff may have access to PNC data within the course of their work.

2.3 Prisons use PNC for a wide range of risk assessment purposes that help to keep prisons safe and secure places to live and work, and to support rehabilitation. Risk assessments supported by PNC help to keep prisoners, staff, visitors and the public safe. Annex C sets out a list of examples of current uses of PNC information.

3. Outcomes

3.1 Compliance with police requirements and guidance in respect of PNC equipment (meaning a PNC terminal or any other device used to access PNC applications) and data use by all HMPPS users.

3.2 Prisons with PNC equipment can use it for authorised and lawful purposes.

3.3 Unauthorised and unlawful use of PNC equipment and data is prevented.

4. Requirements

4.1 Governors of prisons with access to PNC using terminal equipment must ensure that their staff comply with the latest requirements and guidance from the police (Annex A) and set out in this framework. This includes any requirement to audit, monitor or control PNC use.

4.2 Any HMPPS employee handling information held on or extracted from PNC must do so lawfully and in accordance with any relevant police requirements and guidance in force at the time, and any requirements and guidance set out in this framework. The consequences of not doing so may include reputational damage to the prison and HMPPS, possible

withdrawal of the PNC service by the police, disciplinary action against the member of staff responsible and, in some cases, civil or criminal sanctions (see Annex B).

4.3 Governors of prisons with PNC equipment must ensure that there are, at all times, sufficient numbers of individual PNC operators and auditors who have been trained and vetted to police requirements in order to meet the establishment's business needs and to allow for contingencies such as staff absence and leaving, or transferring out of, the establishment, taking into account the time it may take for new users to be appointed, vetted by the police and trained.

4.4 Governors of prisons with PNC equipment must appoint a senior manager to take day to day responsibility for PNC in each such prison as the senior point of contact (SEPOC).

4.5 Governors of prisons with PNC equipment must ensure that regular audits take place as set out within the guidance at Annex B.

5. Constraints

5.1 This policy framework is specific to the use of PNC equipment in prisons and the handling of any information derived from PNC by any HMPPS employee for purposes authorised within this framework.

5.2 PNC equipment in prisons must only be used for purposes authorised under this framework and must only be used by persons authorised and trained to do so.

5.3 PNC equipment must not be used to obtain information on any member of the public (including social or official visitors and staff) or for any purpose connected to personnel recruitment, or the management of employees, unless authorised to do so by agreement with the police for specific purposes for the prevention of crime.

5.4 Nothing within this framework must be construed as requiring any person to act in any way that would conflict with the requirements and guidance set out by the police or would conflict with established procedures for the lawful handling of personal information.

6. Guidance

Police PNC guidance

6.1 Governors and PNC users in prisons should always follow the latest police requirements and guidance. Details of the relevant documents and links at the time of publication of this framework or as subsequently updated are set out in Annex A.

HMPPS PNC guidance

6.2 Governors and PNC users in prisons should also follow the guidance at Annex B, which assists and advises on how best to maintain compliance with police guidance and requirements within the prison setting.

Information assurance and data protection

6.3 PNC users should follow established procedures and requirements when handling personal information, including PNC information. Any handling of personal information must always

comply with legislation and regulatory requirements such as the Data Protection Act 2018 and General Data Protection Regulation.

ANNEX A: Police PNC guidance

1. PNC users should familiarise themselves with, and must at all times follow, the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) as provided by the College of Policing (Code of Practice) or the latest code, requirements and guidance issued by the police.

2. Governors and SEPOCs are responsible for ensuring that all PNC users have access to, are familiar with, and follow the Code of Practice and any other documents providing requirements, advice and guidance published for the purpose of supporting PNC.

3. Every person with access to PNC equipment or data is responsible for ensuring that they are aware of, and comply with, police requirements and guidance and this framework.

4. The latest version (at time of publication of this framework) of the Code of Practice may be downloaded from the following address:

   https://www.college.police.uk/article/consultation-pnc-leds-code-of-practice

ANNEX B: HMPPS Guidance for PNC operators, auditors and SEPOC

1. This guidance should be read in conjunction with police guidance referenced in Annex A.

2. The Association of Chief Police Officers (ACPO) owns the data held on the PNC. His Majesty's Inspector of Constabulary (HMIC) is responsible for overseeing the integrity of the system. This oversight covers police forces and extends to other PNC users including HMPPS.

3. For any prison with PNC equipment, the Governor is responsible for ensuring that all relevant staff comply with the requirements and guidance set out by the police (Annex A) and within this policy framework. This includes any requirement to audit, monitor and control PNC use.

4. Every person with access to PNC equipment or data is responsible for ensuring that they are aware of, and comply with, the requirements and guidance set out by the police (Annex A) and within this policy framework.

5. Governors are responsible for appointing a Senior Point of Contact (SEPOC) with day-to-day responsibility for PNC.

6. The SEPOC shall ensure that a list of all authorised PNC terminal operators and PNC auditors is kept and maintained.

7. The SEPOC shall ensure that there are sufficient numbers of PNC terminal operators and PNC auditors who have been trained and vetted to police requirements in order to meet the establishment's business needs. These numbers shall take into account contingencies such as staff absence and leaving, or transferring out of, the establishment, and the time it may take for new users to be appointed, vetted by the police and trained.

8. The SEPOC shall ensure that all operators and auditors and anyone with access to PNC data understands their responsibilities, police and HMPPS PNC requirements and guidance and is aware of the consequences of non-compliance. Such consequences include (but are not limited to)

    a. Reputational damage to the prison, its Governor and to HMPPS generally
    b. Potential withdrawal of PNC services from the prison or HMPPS
    c. In some cases, disciplinary action and/or criminal prosecution

9. The SEPOC shall ensure that PNC audits are carried out according to the schedule agreed with the Police, normally every two weeks.

10. The SEPOC shall provide a report to the Governor on a regular basis to indicate the level of compliance with police requirements and the requirements of this framework.

11. The SEPOC shall ensure that the prison's contingency plans include loss of access to PNC.

Freedom of Information Act (FOIA) and data Subject Access Requests (SAR)

12. PNC data is not held by HMPPS or the Ministry of Justice (MoJ). Any FOIA or SAR for such data should be referred to the Home Office or whichever agency or person is responsible at the time as Data Controller for PNC data.

13. Requests for any other information in relation to use of PNC in prisons that may be sent to the MoJ. Details: https://www.gov.uk/make-a-freedom-of-information-request

Application for authority to access PNC

14. Explicit authority to access the PNC is granted by the PNC Information Access Panel (PIAP), an ACPO-appointed body which deals with access rights and issues as they relate to an organisation's use of the facility.

15. Any prison applying for access to, and authority to use, the PNC will be required to complete a business case and risk assessment for approval by PIAP.

16. For further information on applying for a prison to access PNC see **'Contacts'** below.

Authorised use of PNC

17. PNC must only be used for purposes authorised in the PNC user agreement and in accordance with this framework and the PNC Code of Practice. PNC data and any local operating instructions and security arrangements must not be discussed with, or disclosed to, any unauthorised person, other than as required by law or ordered by a court.

18. PNC must not be used for any purpose that has not been explicitly authorised in the user agreement with the police.

19. PNC data must only be copied, printed or transmitted electronically if authorised as part of the user agreement. Where any prints or copies are made, such prints must be handled strictly in accordance with the relevant user agreement.

20. Examples of authorised prison uses of PNC data include, but are not limited to, the uses listed in Annex C.

21. PNC must never be used to find information about any member of the public, for instance for the purposes of screening visitors, or for finding information about any member of staff, or when recruiting staff, or any contractor, or any other person who might need access to the prison for official or business purposes, unless authorised to do so by agreement with the police for specific purposes for the prevention of crime.

Contacts

HMPPS PNC Enquiries:	PNCenquiries@justice.gov.uk
PNC customer support:	PNC.Customer-Support@homeoffice.pnn.police.uk

ANNEX C: Examples of current uses of the Police National Computer

(This list is not exhaustive and there may be other authorised uses)

- Security categorisation of prisoners
- Allocation of prisoners
- Completion of cell-sharing risk assessments (CSRA)
- Management of self-harm and suicide risks
- Management of prison transfers, external prisoner movement of all types and hospital bed watches, including completion of the Person Escort Record (PER)
- Management of security intelligence
- Management of purposeful activities
- Allocation of prisoners to appropriate offending behaviour programmes
- Allocation of prisoners to appropriate employment training programmes and work placements in the community
- Allocation of prisoners to appropriate drug and alcohol use reduction programmes
- To support the Category A assessment and management processes
- To support the Escape List assessment and management processes
- To support victim liaison services and policy
- Management of foreign national prisoners
- Management of indeterminate sentence prisoners
- To support the referral process and sectioning procedure under the Mental Health Act
- To support the referral process and removal of foreign national prisoners
- To support the completion of bail information reports
- To support the post-release monitoring process
- To support the completion of pre-sentence reports for the courts
- To support the sentence planning process
- Allocation of prisoners to appropriate sex offender treatment programmes
- To assist in the consideration of post-release probation options, for example allocation to hostels, specialist treatment providers or clinics
- To assist in the consideration of both temporary and longer-term releases on licence and any subsequent licence failure and recall to prison
- To support ongoing risk assessment in relation to the Offender Assessment System (OASys)
- To support ongoing risk assessment in relation to Multi-Agency Public Protection Arrangements (MAPPA)
- To assist in the consideration of non-custodial sentencing options, for example Home Detention Curfew (HDC)
- To support the Parole Board process
- To assist in the identification of civil orders which may have been imposed and are therefore included on the prison PNC print
- Any other authorised and lawful purpose that requires an assessment of risk