

Lincolnshire Police

Policy Document



Police National Computer (PNC) policy PD128

Policy document information

Reference number:	PD 128
Policy sponsor:	ACC
Policy owner:	Head of FCR
Author:	Insp Hodgson (Amy Everest – PNC Supervisor)
Publication date:	October 2024
Review date:	October 2026

Version history

Version	Date	Reason for issue
9	October 2020	Biennial Review
10	October 2022	Biennial Review
11	October 2024	Biennial Review
12	January 2026	Addition of Appendix 13 – NPCC LED and Remote Access Policy

Code of Ethics

All staff involved in carrying out functions under this policy and associated procedures and appendices will do so in accordance with the principles of the Code of Ethics. The aim of the Code of Ethics is to support each member of the policing profession to deliver the highest professional standards in their service to the public.

Legislative compliance

This document has been drafted to comply with the principles of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the staff and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010 and meet our legal obligation in relation to the equality duty. In addition, Data Protection, Freedom of Information and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

Other legislation/law which this policy has been drafted to comply with:

- [Human Rights Act 1998 \(in particular A.14 – Prohibition of discrimination\)](#)

- [Equality Act 2010](#)
- [Crime and Disorder Act 1998](#)
- [H&S legislation](#)
- [Data Protection Act 2018](#)
- [Freedom Of Information Act 2000](#)
- [Criminal Justice and Public Order Act 1994](#)
- [Regulation of Investigatory Powers Act \(RIPA\) 2000 Act](#)
- [Copyright, Designs and Patent Act 1998](#)

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes

Authorised Professional Practice (APP)

This policy has been checked against APP and there is none in relation to the subject matter of this policy.

1. Policy aims (Purpose)

1.1. The aim of this policy and its associated documents is:

- To standardise the use of the PNC across the Force;
- To provide set procedures when accessing, printing, disclosing and retaining information as well as the ongoing management of the PNC.

1.2. The Police National Computer (PNC) is a national database of information available to all forces/agencies throughout England, Scotland, Wales, Northern Ireland, the Channel Islands and British Transport Police. It facilitates investigations and sharing information of both national and local importance. It affords mission critical services to the police, UK Law Enforcement and criminal justice agencies throughout the United Kingdom.

- 1.3. This policy and associated appendices detail what information is available from PNC, how the data should be updated and the various ways it can be accessed, including via Mobile Data terminals (MDTs). It also details how PNC can be used for the transmission of messages both internally and to other Force's via the Broadcast Scheme and the protocols in place to safeguard the disclosure of any information.
- 1.4. This policy is required to ensure the use, access and disclosure of PNC held data by Lincolnshire Police, is lawful and conforms to the legal and regulatory requirements of:
- Computer Misuse legislation 1990
 - PNC Code of Connection,
 - Management of Police Information Guidance 2010
 - National PNC Operating Rules
 - Association of Chief Police Officers (ACPO) PNC Compliance Strategy

2. Policy statement (Key information)

2.1. Origins

- 2.1.1. The efficiency of the criminal justice system and the effectiveness of the police depend upon the accuracy of the PNC records. The PNC is one of the most significant investigative tools available to the service. Its national remit is to provide direct and immediate access to data across the Police Service as well as to the criminal justice service and non-police agencies.
- 2.1.2. The PNC is the only full time operational national police computer system routinely supported by data from all police forces. It is also the prime source of record keeping in relation to the nominal record of offenders and arrestees being processed by the police, the courts and the non-police prosecuting agencies. It also safeguards against unlawful use or disclosure of information by compliance with legal and regulatory requirements.

2.2. Principles

- 2.2.1. The general principles of the policy are to ensure information is correctly and promptly submitted to PNC which in turn allows the most accurate and up to date intelligence to be provided to police officers and police/G4S staff when legitimately requested for policing purposes. It also safeguards against unlawful use or disclosure of information by compliance with legal and regulatory requirements.

3. Other related documents and appendices

3.1. Appendices:

- Appendix 1 – PNC Flow Chart
- Appendix 2 – General PNC Procedures
- Appendix 3 – Blocked Vehicles
- Appendix 4 – Recordable offences
- Appendix 5 – Audit & Monitoring
- Appendix 6 – PNC Access x 3
- Appendix 7 – PNC Broadcast
- Appendix 8 - NPCC PNC Record Deletion Process (Guidance)
- Appendix 9 – Supply of information to private police/other organisations
- Appendix 10 – Training
- Appendix 11 – Mobile Data
- Appendix 12 - General Principles for Officers Circulating Wanted Suspects on PNC
- Appendix 13 - NPCC LED and Remote Access Policy

Related documents:

- PNC Manual
- Health and Safety – Use of Handheld Mobile Data Terminals
- Force Security Policy PD 55
- Force Risk Management Policy PD 122

- Mobile Data Policy PD 219
- Email Archive and Retention Policy PD 146
- Social Media Policy PD 174
- Remote Access operating procedure PD 147
- Protecting Data stored on portable media PD 139

4. Monitoring and review

- 4.1. The Head of FCR is responsible for this monitoring this policy and will determine the PNC strategy for the Force as well as ensuring it is kept up to date and/or amended in the event of any significant changes to PNC Operating Instructions.
- 4.2. This policy is owned by the Head of FCR. It will be reviewed every two years and the Policy will be amended to adopt any good practice from other Forces or to reflect changes in Legislation in the interim period.

5. Who to contact about this policy

- 5.1. Any enquiries about this policy should be directed PNC Supervisor Amy Everest, Tel 01522 558815, Amy.Everest@lincs.pnn.police.uk