

Lincolnshire Police

Policy Document



Force systems misuse policy PD 265

Policy document information

Reference number:	PD 265
Policy sponsor:	DCC
Policy owner:	Head of Professional Standards
Author:	DI Anti-Corruption Unit
Publication date:	July 2025
Review date:	July 2027

Version history

Version	Date	Reason for issue
1	Oct 2023	New Policy
2	July 2025	Review of 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](#)
- [Equality Act 2010](#)
- [Data Protection Act 2018](#)
- [Freedom Of Information Act 2000](#)
- [Legislation - HSE](#)

- [UK GDPR guidance and resources | ICO](#)
- [Computer Misuse Act 1990 \(legislation.gov.uk\)](#)
- [Official Secrets Act 1989 \(legislation.gov.uk\)](#)
- [The Police Regulations 2003 \(legislation.gov.uk\)](#)
- [The Police \(Conduct\) Regulations 2020 \(legislation.gov.uk\)](#)
- [Home Office guidance on police misconduct \(publishing.service.gov.uk\)](#)
- [Investigatory Powers Act 2016 \(legislation.gov.uk\)](#)
- [The Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-keeping Purposes\) Regulations 2018 \(legislation.gov.uk\)](#)
- [Code of Practice for the Police National Computer \(PNC\) and the Law Enforcement Data Service \(LEDS\) \(accessible\) - GOV.UK \(www.gov.uk\)](#)

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. Lincolnshire Police has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by Lincolnshire Police.

Those provisions are shown in the links below and can be accessed via the home page of the APP website:

[Management of police information | College of Policing](#)

[Professional standards | College of Policing](#)

1. Policy aims (Purpose)

1.1. Background Information

- 1.1.1. Police Information Systems contain highly sensitive data. Misuse of such systems will often involve breaching the privacy rights of members of the public and poses a significant risk to the integrity of the police service. The

standards of behaviour and the integrity of those who work within the police service are constantly under scrutiny. It is imperative that the public have confidence in the integrity and impartiality of the police service, and it is the responsibility of Lincolnshire Police Staff to maintain and build public confidence in the police service.

- 1.1.2. Where Lincolnshire Police Staff abuse their position and view information, confidential or otherwise, without a 'Policing Purpose' this serves not only to undermine the trust of the public but is also a breach of the Data Protection Act 2018, the Computer Misuse Act 1990 and The Standards of Professional Behaviour.

1.2. Purpose

- 1.2.1. This policy applies to all Police Staff and its purpose is to safeguard the confidentiality, integrity, and availability of our information. The policy clearly sets out expectations and identifies what Police Staff can and cannot do when accessing Lincolnshire Police/OPCC systems, regarding acceptable use of ICT systems or devices that gain access to sensitive information on local and national databases.
- 1.2.2. This policy will provide clear guidance around what constitutes a legitimate policing purpose, set conditions for use of all Lincolnshire Police infrastructure, make mention of onward disclosure, highlight the responsibilities of all Lincolnshire Police Staff, and detail the ACU assessment process, which includes the potential outcomes for those that fail to follow this policy.
- 1.2.3. This policy supports the organisations values and behaviours and is underpinned by procedures designed to provide clear, definitive and unambiguous direction for all those involved.

2.1. Lincolnshire Police Infrastructure

- 2.1.1. Lincolnshire Police infrastructure, including but not limited to ICT equipment, (e.g. Desktops, Laptops, Phones, Servers etc.) software, applications, operating systems, storage media, networks, data and

information are the property of Lincolnshire Police. These systems are to be used for policing purposes in serving the interests of the organisation.

2.2. Personal Use

- 2.2.1. Personal use of police information is not permitted. Personal use includes but is not limited to the use of the information for the purpose of which is for personal enjoyment, private gain, an advantage or an outside endeavour not related to an organisational business interest.

2.3. Definitions

- 2.3.1. Police Information Systems refers to any system or device that contains personal or other sensitive data (e.g. NICHE, Police National Computer (PNC), Police National Database (PND), Genie, Guardian, etc...).
- 2.3.2. In this policy 'Police Staff' means police officers, special constables, police staff, volunteers, OPCC staff, agency workers or any other person attached to Lincolnshire Police on a temporary or permanent basis whether in receipt of payment or not.
- 2.4.1. The definition of legitimate 'Policing Purpose' is governed by the Management of Policing Information (MoPI) Code of Practice and should be one of the following:
- Protecting life and property
 - Preserving order
 - Preventing the commission of offences
 - Bringing offenders to justice
 - Any duty or responsibility of the police arising from common or statute law

3. Conditions

The following conditions apply to the use of any Police Information System, whether past, current, or future but also apply to any other Lincolnshire Police database, system or device:

- 3.1.1. Any search or enquiry must be justified as being for a policing purpose. This includes the legitimate accessing of information to supply to other agencies such as details of vulnerable victims or witnesses etc.
- 3.1.2. The access must be a part of your normal role. Conducting an enquiry in relation to a reported crime or incident clearly falls within the prevention and detection of crime, when, all other conditions within this document are met.
- 3.1.3. Lincolnshire Police Staff may still have access to Police Information Systems or other databases/systems which are not required for their primary role, such as members of Learning and Development (L&D) and OPCC. In certain instances, there are opportunities to undertake secondary duties, such as police shift staff, which would require access to police systems or databases. Under no circumstances should access be made unless a policing purpose is present.
- 3.1.4. Researching, searching or accessing record(s) out of curiosity, particularly where it involves looking at information regarding yourself, family, friends, acquaintances, neighbours, high profile cases or 'celebrities' is not permitted in any circumstances.
- 3.1.5. You must NOT search Police Information System or any other system/database in relation to yourself, your relatives, your friends or the area where you live, even if you believe that there is a legitimate policing purpose for this. Where a perceived need arises in these circumstances, you must discuss this with your line manager. They must then establish if the need is legitimate and if so, who should carry out the transaction. Where doubt arises, advice must be sought from the ACU. A record of any decision or action must be kept by yourself and your manager and be able to be produced should there be any questions in relation to any actions carried out. Remember it is your responsibility to maintain your integrity. ACU must be notified if you access such a record.

- 3.1.6. It is important to differentiate between Police Staff civilian records and work records on Niche. Your work record will have a collar number assigned and should only have occurrences linked to it that occurred during the course of your policing duties (e.g. assaulted during an arrest). Your civilian Niche record should only have occurrences and other details linked that refer to events that did not occur during your policing duties (e.g. home address burgled). However, it has been found that recording errors do occur on Police systems and there are examples where occurrences, address etc. have been linked to the wrong Niche record. For example, an assault whilst making an arrest may be linked to an officer's civilian record. If you find that something like this has happened to yourself or a colleague, you must notify a supervisor to request that the error is corrected and make a record of how you identified the error.
- 3.1.7. If you inadvertently access information regarding a relative or acquaintance, you have not necessarily done anything wrong. However, you must cease immediately any further research and draw this to the attention of a supervisor who will ask for another officer or colleague to conduct the research. In the rare occasion that no other alternatives exist (i.e. an emergency), the supervisor may authorise your continued use providing it is for a policing purpose and not in significant conflict with the other conditions of this policy. The manager and you should make a record of this request and the decision made and ACU must be notified.
- 3.1.8. It is accepted that Investigators may take an initial look at custody records relating to their assigned area at the start of their shift. This will be in order to ascertain what work may be allocated to them and assist in organising workload priorities. Accessing custody records beyond the minimum to ascertain allocation is not permitted without prior approval from a supervisor who will make a record of that approval detailing why it is appropriate for the Investigator to continue. The Investigator should also make a record of this request and the decision made by the supervisor.
- 3.1.9. If you are a Reporting Person or Victim accessing any record on a force system containing information relating to that report/incident, such an action would not be permitted. If you inadvertently access information regarding or relating to that report or incident you must cease any further research

immediately, make a record of what has occurred and inform your supervisor immediately. ACU must be notified.

- 3.1.10. Where you are a Reporting Person or Victim and a witness statement is required, it should be obtained by Investigating Officer(s). If you create a self-written statement, it should be submitted to the Investigating Officer. Under no circumstances should you attach a statement, exhibit or any other document to the investigation.
- 3.1.11. Where supervisors are approached to authorise a search of a Data System, the supervisor must make a considered decision as to whether it is appropriate for the staff member to continue with their enquiry. If necessary, they should seek advice from ACU. A record must be made of the decision taken by the supervisor and the member of staff.
- 3.1.12. If you are tasking a person or are asked to search any system, confidential or otherwise, on behalf of yourself or another, you and the requester must make a record of the request. This is to ensure that you and the requester can justify your activity in the event you are asked to provide your policing purpose, at a later date.
- 3.1.13. Lincolnshire Police staff are provided training on the use of Police Information Systems and there is a plethora of user guidance available on the Intranet. All Lincolnshire Police Staff must adhere to the guidance/training provided and must not deviate from the process. For example, you must not perform a person search for your own details or those of your colleagues (e.g. name/ DOB etc.) on Niche as part of your daily business, such as allocation of tasks, writing statements etc. All searches concerning any Lincolnshire Police Staff must be undertaken via the officer/unit tab as instructed by L&D and documented in the guidance unless there is a policing purpose to access their civilian record. There is no legitimate reason for any member of Lincolnshire Police Staff to type their own particulars into a person search.
- 3.1.14. It is acknowledged that sometimes members of staff become aware of information that relates to someone personally known to them which they perceive may need police action. In these circumstances the member of staff should tell a supervisor as soon as practicable. The supervisor can

then action it appropriately. Do not research and action the information yourself.

4. Prevention of Misuse

Lincolnshire Police retains an absolute right of access to all information held or processed on any of its ICT systems, without notice.

4.1. Recording and monitoring principles

- 4.1.1. The force records and retains information in line with the records management policy.
- 4.1.2. The Investigatory Powers Act 2016 (IPA) establishes a basic principle that communications may not be intercepted without consent and ensures compliance with ECHR and fundamental freedoms.
- 4.1.3. The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 make an exception to IPA and allow businesses (including public authorities) to intercept communications transmitted across their systems without consent for certain purposes.
- 4.1.4. The monitoring of communications will be considered on a case-by-case basis.
- 4.1.5. Recording and monitoring of systems is used to:
 - Review standards of training or service delivery
 - Review standard operating procedures or Force policy, procedures or guidance
 - Ascertain compliance and demonstrate that the required standards are maintained
 - Ascertain compliance with regulatory or self-regulatory practices or procedures
 - To prevent or detect crime
 - To investigate or detect unauthorised use

- To instigate criminal or disciplinary proceedings
- In the interest of National Security

4.1.6. Lincolnshire Police Anti-Corruption Unit is authorised to carry out the appropriate auditing on ALL Lincolnshire Police Staff on ALL system and device use.

5. Information Security – Onward disclosure

- 5.1. Lincolnshire Police Staff are reminded that disclosure is defined by the Oxford Dictionary as: “the act of making something known or public that was previously secret or private”.
- 5.2. Almost all the information gleaned from Police Information Systems would fall within this definition if it were to be disclosed to anyone who did not have a policing purpose to know, with very few exceptions, regardless of the method of delivery. It is the responsibility of all Lincolnshire Police Staff to safeguard the information and details that they are privileged to.
- 5.3. It is important to remember that fellow Lincolnshire Police Staff do not automatically qualify as having a policing purpose, even if they work within the same department as you. Therefore, you must not disclose police information to colleagues unless there is a legitimate justification for them to be disclosed to.
- 5.4. Due care must be taken when using telephones, radios, voicemail, answering machines, facsimiles, emails and recording equipment or when attending briefings/ meetings to ensure the protection of information sensitive or otherwise. All telephone/radio users must be aware that any speech over the telephone is at risk of interception by unauthorised persons or groups. All staff must comply with the Force’s Information and Data Protection Policies.
- 5.5. It is important that before you conduct a telephone/radio/in person conversation in an open plan office area or outside of the Force’s premises, you must consider the nature of the topic you are about to discuss. If the conversation is of a sensitive nature, you must ensure that there is no

possibility of eavesdropping. Remember to always be aware of who is around you when holding a confidential conversation. In addition, messages containing sensitive policing information must not be left on voicemail and answering machines.

6. ACU Procedural Statement

- 6.1. Over the last few years, Lincolnshire Anti-Corruption Unit has experienced an increase in Misuse of Police Systems cases. This uplift may directly coincide with an increase in ACU proactive capabilities to detect such misuse.
- 6.2. There is a requirement to streamline Lincolnshire Police procedure and assessment process including adopting a 'risk based' process (low, medium or high risk). Cases that are risk assessed as low may be subject to Practice Requiring Improvement (PRI) procedures or Management Intervention rather than defaulting to a criminal or misconduct investigation.
- 6.3. A 'low risk' breach is determined by reference to a number of mitigating or aggravating factors which may include, but not limited to, accidental access or collateral intrusion, where appropriate steps taken to bring to the attention of a supervisor; limited access (e.g. not sensitive personal data) and a one-off instance. In these circumstances it is less likely that the investigation will proceed to a criminal/misconduct/gross misconduct investigation.
- 6.4. A 'medium risk' breach is determined by reference to a number of factors which may include for example, but not limited to, repeated intrusion, even of data which is not sensitive; disregard of policy/safeguards; access to sensitive data even if one-off; failure to take appropriate steps to bring to attention of a supervisor; deliberate unauthorised intrusion (without malicious intent); access to data with personal relevance or significance. In these circumstances it is more likely that the investigation will proceed to a criminal/misconduct/gross misconduct investigation. A medium risk breach may also lead to a vetting review, which could result in the downgrading or withdrawal of police vetting.

- 6.5. A 'high risk' breach is determined by reference to a number of factors which is usually apparent when there has been a deliberate unauthorised access to live criminal investigations; disclosure of information to third parties outside of the organisation; deliberate unauthorised access to sensitive information; unauthorised intrusion for gain (whether financial or otherwise); unauthorised intrusion with the potential to interfere with investigations of crime, complaints or other. In these circumstances it is highly likely that the investigation will proceed to both criminal and gross misconduct investigations which could result in a prison sentence, dismissal from the force and inclusion on the Barred or Advisory list. A high-risk breach will likely lead to a vetting review, which could result in the downgrading or withdrawal of police vetting.
- 6.6. This method of assessment adopts guidance from the College of Policing, specifically 'Guidance on outcomes in police misconduct proceedings'.

NOTE: the examples above are not exhaustive, each breach will be considered on a case-by-case basis, but the approach will reflect the principles set out in Home Office Guidance on police misconduct.

7. Compliance

Compliance to this policy is mandatory and any such breach or suspected breach will be forwarded to and assessed by the Anti-Corruption Unit in line with Misconduct Procedures.

8. Other related documents and appendices

- 8.1. Appendices and related documents.

- Police Staff Code of Conduct
- Police Staff Disciplinary Procedure
- Police (Conduct) Regulations
- Information Audit and Procedures Policy (PD 135)
- Professional Standards Public Complaints and Misconduct Policy (PD 21)

- Protective Monitoring of Lincolnshire Police ICT Systems (PD 194)
- Force Security Policy (PD 55)
- Data Protection & Freedom Information Policy (PD 141)
- Lawful Business Monitoring Policy (PD 258)
- Management of Police Information Policy (PD 118)
- Mobile Data Policy (PD 219)

9. Monitoring and review

- 9.1 ACU are responsible for monitoring and reviewing the policy. This policy will be monitored for accuracy and reviewed yearly.

10. Who to contact about this policy

- 10.1. This policy is owned by the Head of the Professional Standards Department (PSD). However, any questions, queries or comments should be directed to Detective Inspector of ACU in the first instance.