

Lincolnshire Police

Policy Document



Information sharing policy PD 132

Policy document information

Reference number:	PD 132
Policy sponsor:	Deputy Chief Constable – Chris Davison
Policy owner:	Head of IMU – Jen Johnson
Reviewer:	Data Protection Supervisor, IMU – Jana Randle
Publication date:	October 2025
Review date:	October 2027

Version history

Version	Date	Reason for issue
8	Oct 17	Annual Review
9	May 2018	Legislative compliance change to DPA 2018 and GDPR
10	Oct 19	Biennial Review – Minor amendments made.
11	Oct 21	Biennial Review – Minor amendments made.
12	Oct 23	Biennial Review – ‘one-off’ request process updated. Minor amendments made.
13	Oct 25	Biennial Review

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](#)
- [UK General Data Protection Regulations \(UK GDPR\)](#)
- [Data \(Use and Access\) Act 2025](#)
- [Code of Practice on the Management of Police Information, made under Sections 39 and 39A of the Police Act 1996 and Sections 28, 28A, 73 and 73A of the Police Act 1997](#)

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes

Authorised Professional Practice (APP)

APP is developed and owned by the College of Policing (the professional body for policing) and can be accessed online. It is authorised by the College of Policing as the official and most up-to-date source of policing practice. The range of subjects covered by APP is growing all the time.

It has the same legal status as previous guidance; it is not the law and so, while Police Officers and Staff are expected to have regard to APP in discharging their responsibilities, the status of APP is advisory. There may be circumstances when it is legitimate to deviate from APP, providing there is a clear rationale for doing so.

This Policy has been checked against APP, Lincolnshire Police have 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:

<https://www.app.college.police.uk/app-content/information-management/sharing-police-information/>

1. Policy aims (Purpose)

To provide instruction and guidance to Lincolnshire Police Officers and Staff in relation to information sharing, so that we operate within the law, as set out within the Code of Practice, and in accordance with national guidance. This policy relates only to the sharing of **PERSONAL, SENSITIVE** and **SPECIAL CATEGORY/ CRIMINAL** information.

Formal information sharing should be seen as an opportunity to improve performance and reduce risk at all levels, within and across all police forces and the wider 'people protection' community. With the intention to protect the public, in particular children and vulnerable adults, and to assist in the overall cohesion of society.

2. Policy statement (Key information)

The principles and scope of the policy

The Management of Police Information (MoPI) Code and Guidance has been incorporated into the Authorised Professional Practice (APP). The APP is designed to provide a common framework for the Management of Police Information which includes the requirements for the formal sharing of information with identified partners, and for 'one off' requests for the sharing of police information.

The Police Service shares a common purpose for managing information which means that forces can share information with one another **without**

the use of Information Sharing Agreements. It is important, however that there is an audit trail of the identity of the person requesting the information, and the information being shared.

Police information is information that is required for a policing purpose, and within the initial phase of the national IMPACT programme, will come from information held within the following business areas: Crime; Intelligence; Domestic Violence; Child Abuse investigation; Firearms revocations and refusals, and Custody.

Policing Purposes are defined as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offender to justice, and
- Any duty or responsibility arising from common or statute law.

Lincolnshire Police are fully committed to being compliant with the Authorised Professional Practice (APP) and Guidance on the Management of Police Information within the identified timescales.

Information sharing refers to the processing of information either on an ongoing regular basis between partners, or as a one-off request, for the purpose of achieving a common aim. Effective policing relies on the Police communicating and sharing information with a wide range of partners. Information sharing in the context of the Management of Police Information relates specifically to **personal, sensitive and special category/criminal data only** – it does not include statistical data such as crime figures.

Information sharing:

- Is a two-way process that enables links to be made between people, objects, locations and events that would not be possible otherwise;
- Can help deliver improved public services, and protection;
- Leads to an increased openness among partners, which, in turn, build confidence and trust in the Police Service;

- Increases expertise, professionalism and an understanding of the process of sharing information;
- Enables partners to make informed decisions about how best to protect the public.

Information will not be shared as a matter of routine. Each request for information must be viewed individually, with informed decisions made about whether or not to share information. The decision-making process will be documented. Any information shared will be proportionate and necessary for the purpose for which it is being shared.

The sharing of police information falls within three distinct groups:

- Those required by or under statute (statutory obligation) i.e. Court Orders, disclosures to the Child Support Agency, and the Disclosure and Barring Service;
- Those permitted by or under statute (statutory power) i.e. Section 47 of the Children Act 1989 allows for Social Services to request information for ongoing child protection enquiries, and
- Those made under common law to support the policing purposes.

Regular Requests

Information Sharing Agreements (ISAs) will be drawn up where a regular exchange of personal information is required, between the police and identified partners, for a policing purpose.

Agreements will be drawn up by or in consultation with the force ISA Officer when a need for information sharing has been identified. In general terms, the Partner Agency Disclosure Officers (PADO) within the Information Management Unit (IMU) will deal with requests for personal information from identified partners. Requests completed by the PADO team will be uploaded and stored on Niche. The Data Protection Supervisor within the Information Management Unit is the identified Single Points of Contact (SPoC) for ISAs that are dealt with by the PADO team. Additionally, some ISAs, relative to Sectors/ Departments, will identify the Sector/ Department

Inspector as the SPoC or person delegated by them. All 'authorised' ISAs will identify the contact details of the Police and Partner SPoC.

ISAs are used to formalise arrangements between Lincolnshire Police and identified partners. They identify the types of information to be shared and under what circumstances, the SPoC for each party **is** signed off at an executive level by the police and the identified partner(s). A senior member of staff, such as the Senior Information Risk Owner (SIRO), a Chief Superintendent or a person delegated by them, should sign the agreement. In partner agencies, the signatory should also be a senior member of staff who can be held accountable for the processing of information.

Once authorised by a SIRO/Chief Superintendent/ Departmental Head, ISAs will be published for the benefit of the force on the Intranet site.

The Information Sharing Officer within the Information Management Unit at Force Headquarters will maintain the 'master' library of authorised ISAs.

For requests completed outside of the IMU the identified Police SPoCs will maintain a file which will hold details of all requests and responses to requests for information together with a copy of the ISA. During regular reviews by the SPoCs any information contained within the file that has been dealt with and no longer required, **will be retained for six years** from the date of provision of the information. This timescale meets minimum MoPI requirements and also meets the timescale allowable for civil claims. The identified partner SPoC will also maintain a similar file.

All documentation in relation to Information Sharing Agreements will be appropriately marked in accordance with the Government Security Classification (GSC) See PD 228 for further details. For further details regarding the storage of documents please see the Force Government Protective Marking (GPMS) Policy (PD119) and the Government Security Classification Policy (PD228).

‘One -off’ requests

On occasions there may be the need to share information for a policing purpose with an agency or organisation. Where a formal ISA has not been drawn up, this will be dealt with as a ‘one-off’ request.

In general, one-off requests will be directed to the Information Management Unit where they will be dealt with by the Partner Agency Disclosure Officers (PADO). Personal Information will only be provided if the sharing of information meets a policing purpose and the identity of the requester has been verified. Requests and responses dealt with by the PADO team will be documented using a P698A (at Appendix A) & Disclosure of Police information form and will be uploaded and stored on Niche.

Lincolnshire Police officers or Staff, who wish to provide a one-off disclosure to a Partner Agency, should seek advice from the Information Sharing Officer prior to release. In certain circumstances this type of disclosure will be acceptable.

Prior to making a one-off disclosure, the Lincolnshire Police Officer or Staff will be advised to take into account the following considerations:

1. The policing purpose of the disclosure;
2. Proportionality of the disclosure;
3. Necessity and relevancy of the disclosure;
4. How will the disclosure be shared in a secure manner;
5. Recording of the disclosure, to ensure that it is held within the corporate knowledge of the force (e.g. on corresponding Niche occurrence or incident log).

If a Lincolnshire Police Officer/Staff identifies that they are making ‘one-off’ requests to the same Partner on a regular basis they should inform the Information Sharing Officer. The Information Sharing Officer in conjunction with the Lincolnshire Police Officer/Staff will consider whether an Information Sharing Agreement is required.

Considerations when sharing personal information

Police information must be accurate, it must remain relevant to the purpose for which it is being shared and it must be judged on its own merits. The relevance of a specific record must be decided on a case-by-case basis - i.e. it may not be necessary to share details of all information held about a particular individual, dependent upon the details of the request – what is the purpose for which the information is being requested? Any information shared will be proportionate and necessary for the purpose for which it is being shared.

There may be instances when other information comes to light that makes the first record more relevant – i.e. the age of the victim of a sexual assault may not be apparent from the record of conviction on the Police National Computer (PNC), but may be relevant to the request for information, particularly if there is a large age gap between offender and victim.

Similarly, it may be considered relevant, in certain circumstances to provide the partner agency with information that falls outside the request. For instance, information might be shared about a person who resides or associates with an individual that may help build a more complete picture for the partner agency, such as whether a child is living at the same address as a convicted sex offender.

The relevance of the information provided to the request should be explained, to ensure that it is meaningful without making it difficult to read or understand.

Extreme care and careful consideration should be taken where the disclosure of information includes details of witnesses, victims or complainants. In all such cases, advice should be sought from the Information Sharing Officer and/or Data Protection Supervisor.

Human Rights and the Test of Proportionality

In considering whether to share personal information, a balance needs to be achieved between the protection of an individual's rights and the general

interests of society. Article 8 of the Human Rights Act and the European Convention on Human Rights, states that:

“Everyone has the right to respect for their private and family life, home and their correspondence, and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of: National security; public safety; economic wellbeing of the country; the prevention of crime and disorder; the protection of health and morals; or the protection of the rights or freedoms of others”,

To be compliant with Article 8 of the Human Rights Act (referenced above) the sharing of personal information must meet the test of proportionality.

Sharing personal information will be proportionate if:

- The individual concerned consents to information being shared; or
- The purpose justifies infringing the right to privacy;
- The measures taken to meet the purpose are rational and fair, and
- The means used to share are no more than is necessary to accomplish the purpose.

In relation to determining the proportionality of a disclosure, there is a lower threshold to meet the test of proportionality when sharing factual information than there is for rumours or allegations. Similarly, there is a higher threshold to share personal information about less serious crimes, as there is a lower public interest in this information being shared.

E.g. 1 – Proportionate

There may be a request to share basic information (such as their address and car registration) about a person in relation to a street robbery. It would be proportionate to share this information, due to the seriousness of the crime and the low sensitivity of the information you plan to share.

E.g. 2 – Disproportionate

There may be a request to share sensitive personal information (such as their religious beliefs or sexual orientation) in relation to a parking offence. Based on these facts alone, not only would it be illegal to share this information, but it would also be disproportionate for such a minor offence.

Each request for information must be considered on a case-by-case basis. This ensures that the information to be shared is in the public interest, is proportionate, and necessary to comply with Article 8 of the Human Rights Act. Public authorities (i.e. Local Authorities – County and District Councils) are bound by the same obligations under the Human Rights Act as the police are.

Data Protection Act 2018

The Data Protection Act (DPA) provides a framework for sharing personal information or sensitive personal information in compliance with the six DPA principles:

- Principle 1 – Lawful & Fair
- Principle 2 – Specified, explicit, legitimate
- Principle 3 – Adequate, relevant, not excessive
- Principle 4 – Accurate, up to date
- Principle 5 – Kept no longer than necessary
- Principle 6 – Processed in a secure manner

Schedule 2, Part 1 (2) of the Data Protection Act, creates exemptions to certain data protection principles, where data is processed or shared for the purpose of:

- Prevention and detection of crime;
- Apprehension or prosecution of offenders, and
- Assessment or collection of any tax or duty.

The exemptions apply to certain principles of the Data Protection Act, where the application of those principles would be ‘likely to prejudice’ the purposes referred to above. The exemptions, however, must be applied on a case-by-case basis.

Common Law Duty of Confidence

The common law duty of confidence applies where information of a personal or sensitive personal nature is collected and recorded. A breach of confidence will apply when the information collected and recorded is used in an unlawful manner. There are, however, a number of exceptions to the duty, specifically:

- Where there is a legal requirement (either under statute, or a court order) to disclose the information;
- Where there is an overriding duty to the public (e.g. where the information concerns the commission of a criminal offence or relates to a life-threatening circumstance), or
- Where the individual to whom the information relates has consented to the sharing.

The police also owe a duty of confidentiality to victims and witnesses of crime, who may expect a greater level of privacy than offenders. A balance therefore needs to be struck between sharing such information and the rights of victims and witnesses, and privacy.

Consent does not need to be sought, for example, where the request to share meets a policing purpose and does not compromise operational procedures, or an individual's safety. An assessment of the vulnerability of those at risk and the impact of the disclosure on the individual will need to be made before making a decision whether to seek consent.

In most circumstance consent to disclose personal information is not required as the police and Partners will rely on an alternative lawful basis for disclosure.

If the lawful basis for the police disclosure is consent, this will need to be sought and documented alongside the corresponding request and disclosure form.

Business processes associated with Information Sharing Agreements

Form A (P698A) Request for Personal Information has been designed for use by partners when requesting information. It will identify the subject matter, the information requested, the reason for the request and possible consequences if information is not provided. It will also identify the person requesting the information, their contact details and organisation they represent. Also included is the capability for any information within the request that is not previously known to the police to be submitted via the 3x5x2 system into Lincolnshire Police intelligence system. The form can be sent to the partner SPoC by e-mail.

Disclosure of Police Information forms have been designed for use by the PADO team to reply to requests from various Partner Agencies. The forms are templates which are created and stored in Niche. The form documents the requester's details, the data subject's details and the decision maker's details and allows for a record to be made of the information provided and the date on which it was provided. The completed form is sent via a secure/encrypted messaging system.

Form B (P698B) Response to Request for Information has been designed for use to reply to Form A requests that are not dealt with by the PADO team. The form documents the fact that the provision of police information will meet a policing purpose, or not, and/or a legal requirement, and records that fact, together with details of the decision maker. It then confirms the subject matter and allows for a record to be made of the information provided, or attached thereto (if a computer printout), and the date provided. The form will be sent via a secure/encrypted messaging system.

Form C (P698C) MOPI – Number of items destroyed has been designed for use to record the number of items destroyed. There will be no reference to the subject matter once the Forms A & B have been destroyed.

Form D (P698D) – Explicit Consent form has been designed for use where consent is required before the information can be shared.

Requests/ responses for personal information from Partner Agencies that are dealt with by the PADO team will be recorded and stored on Niche.

Police SPoCs that deal with requests for personal information that fall outside the remit of the PADO team will ensure that all relevant documents are recorded and stored appropriately. The police SPoC will ensure that when a request for personal information is made the Form A and the corresponding Form B will be stored together, in the file created for such purpose. The partner SPoC will maintain a like file.

On a regular basis the Police and partner SPoCs will review the contents of the file. Documentation **will be retained for six years** from the date of provision of the information.

All Forms associated with Information Sharing Agreements are available for download from the Force intranet site. (Home - Library - Forms - P698)

All documentation in relation to the information sharing process will be subject to, and appropriately marked, in accordance with GSC – See Policy PD228. When not being worked upon, all related paperwork should be stored within an appropriate secure environment. The forms A, B, C & D (P698A, P698B, P698C and P698D) are already marked accordingly.

The use of computers, laptops and mobile devices for the movement of police information, should only be directed to secure email sites – not personal email addresses, and should only be undertaken on computers, laptops and mobile devices authorised by the force.

SPoC files for each partner will consists of a copy of the signed off ISA; a copy of **Guidance for SPoCs**; Corresponding collated Forms A & B, and Forms C & D where appropriate.

Review of Information Sharing Agreements

Once 'authorised,' Information Sharing Agreements will be reviewed initially at 6 months, and then annually thereafter. The information Sharing Officer will conduct the review in consultation with both SPoCs to ensure that the ISAs are still fit for purpose to meet the needs of both partners. If

adjustments to the ISA are required, the relevant amendments will be made and a record will be documented. If required, the updated ISA will then replace the existing ISA on the Intranet and the signed copy will be maintained within the 'central library' by the Information Sharing Officer.

Audit

The ISA Officer may undertake an audit of the Information Sharing process associated with a force ISA at any time. However, as a minimum audits of the content of the SPoC's files will be undertaken on a biennial basis and will coincide with the corresponding ISA review. The audit will review whether the forms are being completed correctly and that any contents no longer required after six years has been removed and destroyed. Audits are liable to be subject to inspection by the College of Policing and Her Majesties Inspector of Constabulary (HMIC).

The audit will include the following areas:

- That a copy of the current signed off ISA is retained within the file set up by the police SPoC.
- That Forms A, B, C & D are available.
- That Form A has an entry in relation to 3X5X2 submission from the original information provided, if relevant.
- That the corresponding Form B is filed with the correct Form A and has the 'decision making' process duly completed and signed off.
- That Form C is present and up to date.
- That Form D has been signed by the data subject where necessary.
- That any specific procedures identified are adhered to.

3. Other related documents and appendices

3.1. Appendices

- Appendix A – Form A (P698A)
- Appendix B – Form B (P698B)

- Appendix C – Form C (P698C)
- Appendix D – Form D (P698D)
- Appendix E – Guidance for SPoCs

Related documents

- Force Security Policy PD 55
- GSC Policy PD 228
- GPMS Policy PD 119
- Information Management Strategy
- Review, Retention & Disposal (RRD) Policy

4. Monitoring and review

- 4.1 Subject to any new legislation or changes in case law, which require immediate amendments, this document will be reviewed on a biennial basis by the Force Information Sharing Officer in the IMU.

5. Who to contact about this policy

- 5.1. This policy is owned by the Information Manager, IMU and any enquiries about this policy should be directed to the Force Information Sharing Officer, IMU.