



Information Sharing Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

What this Procedure covers

- Defines Information Sharing and Information Sharing Agreements (ISA);
- Explains information sharing legal requirements;
- Identifies when an Information Sharing Agreement is required;
- Describes the processes that are to be followed to produce Information Sharing Agreements;
- Sharing information outside an Information Sharing Agreement as an ad hoc request;
- What to do when sharing information and ensuring its security

What this Procedure does not cover

- Disclosure of material in connection with criminal proceedings as defined under the Criminal Procedures and Investigations Act 1996
- Guidance about sharing information between police forces for a policing purpose
- Guidance about specific legal regimes such as Subject Access, Freedom of Information and Common Law Police Disclosures (formerly Notifiable Occupations Scheme).

Officers and staff who are in any doubt about how to deal with information sharing issues should not hesitate to seek further advice by contacting their nominated business area's information sharing SPOC, and if further assistance is still required, The Civil Disclosure Unit within Evolve Legal Services.

Overarching Policies:

Force Information Security Policy
Records Management Policy
Data Protection Policy

Procedures:

Protective Marking Procedure
Data Protection Procedure

Freedom of Information Procedure
Review, Retention & Disposal of Information Procedure
DBS Unit Procedure
Data Protection – Subject Access Procedure
Police Evidence in Civil Litigation and Certain Criminal Cases Procedure
Information Audit Procedure
DPIA Procedure

Other Documents:

Multi-Agency Overarching Information Sharing Protocol
Partner Agency Information Sharing Arrangements Form
Information Sharing Process Flowchart
Information Sharing Agreement Template
Information Commissioners Code of Practice
NYP Retention Schedule
Code of Practice & Guidance on the Management of Police Information (MoPI)
College of Policing Authorised Professional Practice Management of Police Information
Information Management – Security Reports.

Process

1. Information Sharing and Information Sharing Agreements - Overview

Information sharing is the disclosure of data from one or more organisations to a third-party organisation or organisations (known as partners). Information sharing can be ad hoc, or regular. An Information Sharing Agreement (ISA) will normally be required where the sharing:

- Is necessary for a policing purpose; and
- Involves personal data as defined by Article 4 (1) of the General Data Protection Regulation ('GDPR'); and
- Is on a regular and ongoing basis; and
- Partners involved in information sharing require an agreement

An ISA is a formal agreement between organisations wishing to share personal information. The Information Commissioner's Office (ICO) recommends ISAs as best practice to govern sharing arrangements. An agreement ensures sharing is lawful and gives officers and staff confidence and practical guidance about how to share appropriately. ISAs also ensure that we are mindful of, and have documented, the relevant compliance towards security and maintaining information management. The key benefits of an ISA are that it can:

- Inspire public trust by helping ensure that legally required safeguards are in place and complied with;
- Afford protection of individual's personal data when their information is shared;
- Encourage greater trust and a better relationship with partners;
- Reduce reputational risk caused by the inappropriate or insecure sharing of personal information;

- Minimise risk of breaches and consequent enforcement action by the Information Commissioner's Office or other regulators; and
- Reduce risk of questions, complaints and disputes about the way North Yorkshire Police shares personal information.
- Assists in evidencing NYP's accountability obligations under the data protection legislation

Please note that Information Sharing Agreements can also be known as Memorandums of Understanding (MoU) or Service Level Agreements (SLA).

Officers and staff should comply with the "sharing" section of the Information Management Authorised Professional Practice and with the ICO Data Sharing Code of Practice which is a statutory code.

2. Information Sharing Powers

The powers for sharing police information can be categorised into three distinct groups:

- Sharing required by or under statute (statutory obligation);
- Sharing permitted by or under statute (statutory power);
- Sharing under common law to support the policing purposes (common law), including information sharing and dissemination with public, private bodies or individuals.

Sharing of police information must be linked to a policing purpose as defined by the APP on information management and included in the special definitions at the end of this document.

a) Statutory Obligation

A statutory obligation is a specific legal obligation to disclose police information to another party, for example Disclosure & Barring Service checks. NYP has separate procedures for each of the following legal regimes and specialist teams to deal with them (please see links above for more information):

- Disclosure & Barring Service (DBS team)
- Civil Court Orders for disclosure (Civil Disclosure team)
- Freedom of Information (Civil Disclosure team)
- Rights of access under the Data Protection Act (Civil Disclosure team)
- Child Sex Offender Disclosure Scheme (MAPPA)
- Serious Crime Teams (SVT teams)

Further information on the operation of these schemes please contact the relevant team.

b) Statutory Power

A statutory power is a specific discretionary legal power, but not an obligation, to share police information with another party. Examples of statutory powers are Article 23 (d) GDPR and Section 2 of Schedule 2 of the Data Protection Act, Article 23 (f) GDPR and Section 5 of Schedule 2 of the Data Protection Act 2018 and Section 115 of the Crime and Disorder Act 1998.

Police officers and police staff should not share information without a legal basis for doing so. Police officers and staff should challenge requests for information where the legal basis for sharing is unclear and seek advice from the Civil Disclosure Unit if in doubt. The National Decision Model helps police officers and staff to examine and challenge decisions and can be used as a basis for assessing

the need to share information. It should also be used for assessing the limited sharing opportunities identified in the Crime and Disorder Act 1998. The Crime and Disorder Act 1998 imposes a duty on chief officers to share information with Crime and Disorder Reduction Partnerships where appropriate.

c) Common Law

Common law is not an unconditional power to share information. Where the police are requested to share information with a partner and a statutory obligation or power does not exist, a policing purpose should be established as the decision to share is risk based. For guidance on what constitutes a policing purpose please refer to the APP Information Sharing Guidance. It should take into account the source of the information, and restrictions on its onward dissemination. This should be balanced against the requirements of the common law duty of confidentiality, the Human Rights Act 1998, the GDPR and the Data Protection Act 2018

There must be a pressing social need to share information. The justification for disclosing personal information to a third party under the common law is considered to be equivalent to that required for disclosing non-conviction information in accordance with the provisions of Part V of the Police Act 1997.

The common law police disclosure provisions allow forces to proactively provide sensitive personal data to a third party i.e. An employer using common law powers. The Civil Disclosure Unit deal with CLPD (which replaced the notifiable occupation scheme)

d) Consent

In certain situations, information will be shared as we have received consent from data subject. The GDPR imposes certain conditions in relation to consent. This includes (but is not limited to):

- Consent is only relied upon when it is the most appropriate lawful basis
- All requests for consent will be made prominent and separate from any other terms and conditions
- A record is kept of any consent received.
- We will regularly review consents received to check that the relationship, processing and purposes have not changed.
- We will ensure that, when the consent relates to a child under the age of 13, the consent is gained from a parent or appropriate adult.

More guidance on the use of consent is available on the Information Commissioner's Website.

Officers and staff wishing to share information under common law police disclosure provisions must seek approval of an officer of at least the rank of Assistant Chief Constable (ACC).

Whichever of the above three information sharing gateways are used, any sharing must also comply with the Data Protection Act, the Human Rights Act and the common law duty of confidence. Brief guidance is contained below, but further advice should be sought from Civil Disclosure in the case of any doubt.

Data Protection

Any information sharing must comply with the principles of the GDPR (for general processing) and the Data Protection Act 2018 (DPA) for law enforcement processing). Information sharing must be lawful, fair and done in a transparent manner. For general processing, conditions laid down in Article 6 and, if applicable, Article 9 GDPR (special categories of personal data) must be met. Processing for law enforcement purposes is only lawful if one of the conditions within s.35(2) of the DPA is met and s.35(3) to (5) must be met for sensitive processing. Officers and staff are referred to the Data Protection Authorised Professional Practice and Information Commissioner's website for full details of how to ensure compliance with the DPA.

Common Law Duty of Confidence

This duty applies where information of a personal or sensitive nature is collected and recorded. A breach of confidentiality applies when the information collected and recorded is used in an unlawful manner. There are, however, a number of exceptions to the duty. These are specifically where:

- there is a legal requirement (either under statute or a court order) to disclose the information
- there is an overriding duty to the public (for example, where the information concerns the commission of a criminal offence or relates to life-threatening circumstances)
- 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 to privacy.

In certain circumstances 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. In most situations, consent will in fact not be appropriate and should not be used as the legal basis for sharing information. This is because, as an organisation we are in a position of power meaning it will be difficult to show that an individual has freely given their consent. Please refer to Information Commissioner's Website for more information.

Human Rights

Forces should ensure that a fair balance is achieved between the protection of an individual's rights and the general interests of society. Sharing personal information may be proportionate if:

- the individual concerned consents to the information being shared, or
- the purpose justifies infringing the right to privacy, and
- 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.

The threshold to meet the test of proportionality when sharing factual information is lower. There is a higher threshold to share personal information about less serious crimes as there is a lower public interest in this information being exchanged.

This means that police officers and staff need to ensure, on a case-by-case basis, that the information they are considering sharing is in the public interest and is proportionate, necessary and meets a legitimate aim under Article 8 of the European Convention on Human Rights (ECHR).

Identifying when an Information Sharing Agreement is required

The Police Service shares a common purpose for managing information. This means that forces can share appropriate information with one another without the use of Information Sharing Agreement.

ISAs are required only when:

- The information being shared involves personal and/or sensitive personal data, (see data protection Authorised Professional Practice for the definitions. Even if the information is neither of the above, it may still be felt that an ISA would be desirable. An example is where more than one partnership agency is providing statistical information into a central point and that information will be disseminated further and could possibly identify an individual e.g. Crime Mapping.
- The sharing is on a regular basis and is required for a policing purpose; or
- Personal data is being shared; or
- Where partners involved in the sharing of information require one.

Before developing a new ISA, check first whether there is a national or local ISA already in place (civil disclosure subsite). If there is one, follow the procedure set out in it.

If no agreements are already in place, there are three possible types of agreement and NYP officers and staff are referred to the Information Sharing Agreement Guidance for SPOCs, CHECK for details of the processes to follow to set up the correct type of agreement depending on the circumstances. The three types of ISA are:

- National ISAs
- Partner Agency Information Sharing Arrangements Forms
- Information Sharing Agreement

The following process does not apply to national ISAs, and for that process officers should contact the Civil Disclosure Unit for further guidance. For non-national ISAs, the process is as follows:

The relevant template should be completed by the relevant business area who is sharing, in accordance with the guidance and prompts within the document, then sent to the Civil Disclosure mailbox. The Civil Disclosure Unit will review the template, advise about any suggested amendments, advise on the legal basis and complete that section of the template accordingly. When the agreement is completed by Civil Disclosure, Civil Disclosure will arrange for consultation with the Information Security Officer and Data Protection Officer.

Once returned, it will be sent back to the officer/staff with ownership of the agreement for the partner agency/agencies to review and sign. Once approved and signed by the partner agency / agencies, the ISA will be signed by the Information Asset Owner. When all parties have signed the agreement, it will be returned to the Civil Disclosure Unit for publication on the subsite & (if appropriate) publication externally in line with the force's publication scheme.

Agreements will be reviewed in accordance with the provisions of each agreement and will be completed by the information sharing SPOC within the business area. A review may be prompted by the Civil Disclosure Unit, or by the SPOC when they become aware of changes.

When considering the necessity for an Information Sharing Agreement, consideration should also be given as to whether a Data Protection Impact Assessment (DPIA) is appropriate. If the information sharing is high risk, then a DPIA may be required. Advice should be sought if any doubt. A DPIA screening questionnaire is appended to the ISA template.

Sharing information outside an Information Sharing Agreement

If you think the information should be shared outside of an ISA, due to it being an ad hoc request, consideration needs to be given as to what the legal basis for the sharing is, whether the sharing is for a policing purpose and whether there are any potential risks or benefits in sharing the information e.g. concern for safety or harm of an individual.

If unsure whether to share the information seek advice initially from the information sharing SPOC within your business area. If you still require advice following discussion with the SPOC, seek advice from the Civil Disclosure Unit. However, if you need to make a decision about whether to share information outside of an ISA and it is not practicable to obtain advice, it is almost always possible to do so without risking a breach of the law if you obtain the consent of the person concerned.

When sharing information outside an ISA make sure that you consider and make a written note (in pocket notebook, policy book, on the case file or some other suitable format to be retained) of the following:

- Who is asking for the information?
- Have you recorded their name, position, organisation and contact details?
- If an e-mail address has been provided, is it a work e-mail address rather than a personal e-mail address?
- Have you verified the identity of the person requesting the information?
- What information is being asked for?
- What purpose will it be used for?
- Is the information being requested personal information?
- Has a statutory or common law provision to share information been established?
- If yes, how do they want the information?
- When do they want the information?
- Record your decision, how you made it and what information was shared

Please Note: Not all information recorded on Force and National systems can be disclosed to a third party. Examples include Motor Insurance or DVLA driver/vehicle data available via the PNC. The Police are not permitted to routinely disclose such information outside the Police Service. Before disclosing any information from a National system to any individual outside the Police Service you should ensure that disclosure is authorised.

What to do when sharing information and ensuring its security

The Information Security Policy should be complied with when entering into any new sharing arrangement.

When sharing information, security handling should be abided with depending on the GSC marking of the information. Please see the Protective Marking Procedure on the appropriate GSC mark that should be placed on the information and how to send the information to the partner agency.

Information should only be shared via e-mail when an official work e-mail address has been provided by the partner agency. Information should not be disclosed to a personal e-mail address.

As part of the requirements of the Code of Practice for the Management of Police Information, the information sharing Single Point of Contact (SPOC) within the area of business identified by North Yorkshire Police will maintain an Information Sharing File in respect of this agreement.

This file (which should be electronic) will contain:

- Record of North Yorkshire Police information disclosed
- Record of information disclosed to North Yorkshire Police
- Decision or justification to disclose or not disclose
- Access and vetting list
- Notes of meetings with partners
- Details of recent correspondence and phone calls
- Record of any review of the agreement

Where NYP Information is held by the partner agency there is the possibility that breaches of security will occur.

There should be appropriate wording within any Information Sharing Agreements in place to instruct such partners as to what to do in the event of any security incident.

Partners should contact their NYP contact in the first instance who will, in turn, contact the Data Protection Officer, Information Security Officer or ICT Service Desk in order to report such incidents and complete the security incident template on the Intranet via e-Forms- Information Management – Security Reports.

It is also important to note that such incidents will be recorded and reported upon, and where it is discovered that any partnership is posing a threat to NYP through repeated incident occurrences, the continuance of such partnerships will be reviewed. Partners will be advised of the outcome of any evaluation.

Training and SPOCs

All officers and staff are required to undertake a mandatory Data Protection MLE package – Managing Information, completion of which will be monitored.

In addition, each business area will nominate a SPOC to act as the information sharing specialist within their area. The SPOCs will receive additional training from the Civil Disclosure Unit on information sharing and related issues and will also be required to complete some additional MLE training packages identified below. In the first instance SPOCs will act as a source of advice for colleagues, and a point of liaison between their business area and Civil Disclosure in complex cases.

Training slides also accompany the multi-agency overarching information sharing protocol and officers and staff involved in setting up information sharing agreements are encouraged to consider those slides.

All information sharing SPOCs within business areas are advised to complete the MLE packages: Managing Information, GSC, Data Protection Foundation and Managing Information Refresher Videos.

Responsibilities

Heads of Service & Safer Neighbourhood Commanders

- Support and encourage staff to be familiar with this Procedure and share information appropriately
- Ensure the process of sharing information is adhered to by both those in a supervisory and user capacity
- Nominate SPOCs and support completion of training detailed above.

Supervisors/Line Managers

- Support and encourage staff to share information appropriately
- Ensure that the decision to share meets a common law or statutory duty or power prior to creating an ISA
- Ensure that information being shared does not compromise any police operation or the safety of others
- Ensure that a risk-assessment process is adhered to by the user when making a decision to share information
- Provide feedback to staff on this topic in the course of normal management activity

Individuals sharing information and business area SPOCs

- Ensure that when personal information is being shared the requirements of the Data Protection Act, Human Rights Act and the common law duty of confidence are complied with
- Follow NYP's policy and procedure in relation to Information Security and Protective Marking
- Record any decision either to share or not to share information
- Ensure that the information being shared is lawfully disclosable under the common law or for a statutory purpose and is proportionate and necessary
- Take responsibility for documenting any new ISA and completing the DPIA screening questionnaire.
- Draft a full DPIA if required.
- Maintain currency of ISAs and their reviews.

The Civil Disclosure Unit, Evolve Legal Services, Data Protection Officer and Information Security Officer

- Provision of legal advice on disclosure/ information sharing
- Provision of advice and guidance for the development of ISAs
- Ensuring all ISAs are held and managed centrally within the force
- Ensure that ISAs are reviewed (annually) in accordance with force policy
- Act as the Information Sharing Contact within NYP as per the multi-agency overarching information sharing protocol.

Definition of Special Terms

Policing purpose means one or more of:

- 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

Personal data is information relating to an identified or identifiable natural person, The natural person is one who can be identified either directly or indirectly by data such as their name, identification number, location, online identifier, or specific factors such as physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special Categories of Personal Data is information relating to an individual's:

- Racial, ethnic origin or religious belief;
- political opinions
- religious or philosophical beliefs or trade union membership;
- genetic and biometric data
- health data
- data concerning a natural person's sex life or sexual orientation
- alleged commission or commission of any offence
- proceedings for any offence committed or alleged to have been committed
- disposal or sentence concerning any alleged or committed offences

SPOC – Single Point of Contact

GSC – Government Security Classification