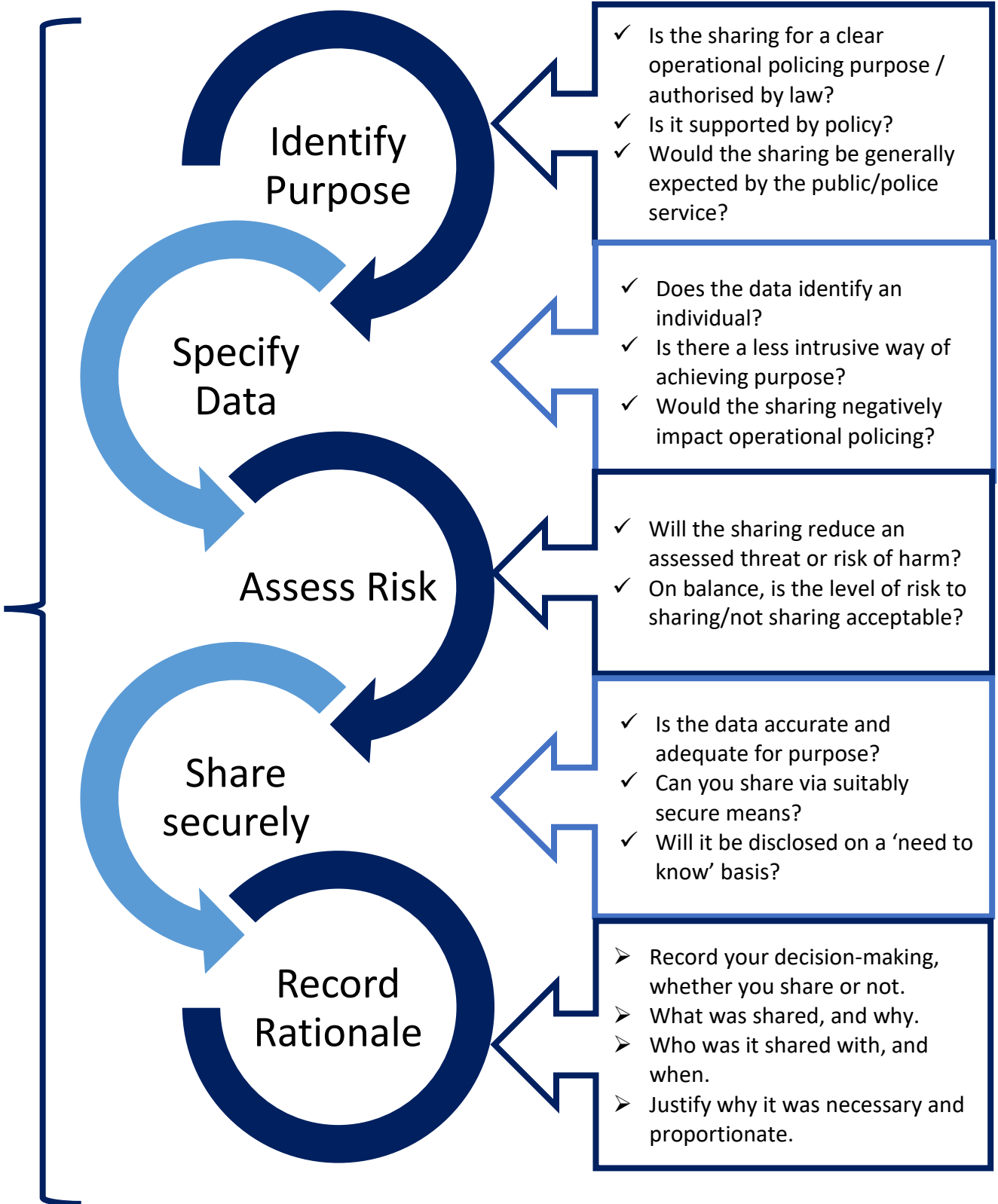


Simple Decision-Making Flowchart

**Consider Code of Ethics**



The below Data Sharing Disclosure checklist provides more detail to help support your rationale. This checklist should also be read in conjunction with detailed supplementary guidance provided by your business area e.g. MASH Early Intervention or Mental Health, where available.

## Share with Confidence Data Sharing Checklist

As officers or police staff, you may from time to time need to share information for policing purposes with other organisations. Where this is part of a reciprocal, repeated, regular sharing of personal data, a purpose specific data/information sharing agreement (DSA/ISA) should be developed and followed prior to the sharing taking place. Alternatively, in the absence of a DSA/ISA, or where the sharing is a **one-off, one-way disclosure** by the police, this checklist should be followed to best ensure the data sharing is lawful, necessary and proportionate.



This checklist is intended to be consistent with the [National Decision Model \(NDM\)](#) and facilitate compliance with data protection legislation.

Sharing information can be very important for safeguarding. The law is there to allow you to share data safely and robustly for this purpose, where necessary and proportionate. The Checklist below sets out factors for officers and staff contemplating the sharing of personal data to consider. There are no right or wrong answers – the considerations on this checklist are to assist with your decision-making rationale.

### 1. Is the data sharing ethical?

- Is this sharing consistent with the [Code of Ethics](#)?
- Would the sharing be generally expected by the public/community or police service?
- Is the sharing for a clear operational [policing purpose](#) (e.g. prevent harm to individuals, prevent or detect crime, or a perceived safeguarding risk to an individual)?
- Could you justify your action or decision if challenged?

### 2. What information is being shared?

- Would the shared information directly identify a living individual, or could the individual be identified indirectly by combining this information with other information available to the recipient (personally identifiable data)?
- Is there a less intrusive way of achieving the purpose without disclosing personally identifiable data? Could you summarise a gist or redact any 'benign' information?
- Are you confident the sharing would not prejudice any ongoing investigations or prosecutions?
- Are you content that the sharing would not reveal operational tactics or intelligence gathering processes?

### 3. Have you assessed threat and risk?

- Are you clear about what you are trying to achieve by the sharing?
- Will your sharing reduce an assessed threat or risk of harm?
- Where needed have you obtained further information or sought advice?
- Have you balanced the potential risk of harm if either you share or do not share?
- Is the level of risk acceptable?

### 4. Do you have the power to share?

- Is the sharing required or permitted by law?
- Is there a pressing social need to share the information in the public interest?
- Would the sharing be consistent with national/local guidance or policies covering this type of situation?

## 5. Options if you decide to share

- What information do you need to share?
  - Only share what is necessary and proportionate.
  - Ensure the data is accurate and adequate to achieve the purpose.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared using suitable/secure means (verbal or written).
  - Ensure you are giving information to a trusted recipient.
  - Disclose on a 'need to know' basis – remove unnecessary third party data.
  - If data shared is found to be inaccurate, recipient should be informed.

## 6. Take Action – Record your decision making

Decision makers are accountable for their decisions and must be prepared to provide a rationale for what they did and why. Whatever the circumstances, the police service recognises that it is impossible to record every single decision and not all decisions need to be recorded. In most cases professional judgement should guide officers on whether or not to record the rationale, as well as the nature and extent of any explanation.

- The record should be proportionate to the seriousness of the situation or incident, and the sensitivity of the information shared, particularly if involving risk of harm to a person.

Good practice is to record your data sharing decision and your reasoning – whether or not you shared the info. If you share information you should record:

- What information was shared, and why (for what purpose).
- Who it was shared with.
- When it was shared.
- Your justification for sharing (why it was necessary and proportionate).

## Summary

Officers and staff should uphold ethical decision making. You should know what information is being shared and why, ensuring it is both necessary and proportionate for a clear policing purpose. Any risks of harm, prejudice to operational policing or significant impact on an individual by sharing (or not sharing) should be assessed.

If after working through the checklist above, you still have serious concerns around whether to share or not, your first port of call should be to discuss with your supervisor. Each force also has dedicated information management teams who can provide data protection advice to support your decision-making.

Just because risks have been identified or the information is sensitive, does not prevent the data sharing. Purpose is key – do you have a clear operational policing purpose for disclosure? In most cases, it will still be reasonable to share the information and make a disclosure as this may outweigh any potential risks – balanced against the risks of not sharing. You will not be penalised for disclosing in good faith, as long as there is a good rationale for doing so and you take the steps above to minimise the data shared wherever possible.

If you have to account for your decision to share information, you should be able to say it was:

- Proportionate, legitimate, necessary and ethical and;
- Reasonable in the circumstances facing you at that time.

By working through the above checklist to help with your decision-making rationale, you should be able to share with confidence.

## Understanding Consent

Both internally within policing and externally with our partners there is confusion on the need for 'consent' in order to share information. In many cases there are misunderstandings as to what 'consent' is referring to – consenting to engage with an organisation, consenting to a referral for services, or reliance on consent as the lawful basis from a data protection perspective?? In order to improve confidence in data sharing, we need to have a common understanding around what is meant by consent as used by our different colleagues and partners.

### **Same Word, Different Meaning**

When Health & Social Care colleagues refer to consent, they tend to mean seeking the views of the family/individual to engage with the organisation, including how they feel about their information being shared with other parties to support this engagement. This, along with obligations under the Common Law Duty of Confidentiality, is embedded in the Health & Social Care legislative framework and important part of their work.

### **What can we do from a Police perspective?**

To allow information given in confidence to be lawfully shared with and by Health & Social Care colleagues, you must evidence how the duty of confidentiality has been set aside – by clearly justifying and stating what express/implied statutory or common law powers are being used. It is also good practice (where this does not prejudice the operational policing purpose) to discuss with the individual – inform them of what you intend to do with their information and why, record their view and whether they are in agreement.

It is important to acknowledge that not wanting their information shared is not a barrier and shouldn't prevent the sharing. Indeed a reticence to engage with other agencies or have agencies share information may indicate an increase in risk so potentially more reason to share. Most people that police interact with are not doing so by choice so their reluctance could be down to an inherent mistrust of police and/or authority.

In most cases consent will not be your lawful basis for processing so you should avoid giving people the impression that their consent is required – raising the subject of consent is likely to mislead! A clear and identified policing purpose (*like preventing a possible safeguarding risk*) provides us with the lawful basis and enables us to share under data protection legislation.

### **What is 'true' consent?**



Consent should be freely given, clear and unambiguous. The individual should have real choice and control with the option to withdraw consent or change their mind at any point, and have their data erased. A clear statement of consent should be recorded.

### **Why is consent not appropriate in most cases within Policing?**



It is not true consent, if there is an imbalance of power between the organisation and the individual, e.g. a police officer and a victim. If it is seen as a precondition to accessing a service, e.g. your crime will not be investigated unless you consent. If you will record the information and act on it regardless of consent, e.g. there is potential safeguarding risk. In most public sector organisations a record must be kept of the interaction with the individual, even if they do not want to engage or accept support offered.

### **What does this mean?**

If you have a clear policing purpose, you know what information is being shared and why, it is both necessary and proportionate and; you have rationalised (and recorded) your decision using the Share with Confidence checklist, **you can lawfully share the information without 'consent'**.