Data sharing in multi-agency meetings

Guidance and example scenarios for homelessness services

Let's end homelessness together

Homeless Link, Minories House, 2-5 Minories, London EC3N 1BJ | 020 7840 4430

www.homeless.org.uk | Twitter: @Homelesslink | Facebook: www.facebook.com/homelesslink

Data sharing in multi-agency meetings

Guidance and example scenarios for homelessness services

Contents

Produced by
The National Practice Development Team with thanks to Nick Swain, Ewa Kapica, Bev Reynolds & Viv Adams.

Published: December 2021

Introduction

This guidance has been written to support voluntary sector organisations working with people experiencing homelessness on issues relating to sharing of client data in multi-agency meetings. It forms part of a suite of Homeless Link resources on effective partnership working[1]. Homeless Link also ran a series of six webinars in 2018 on the (then) new General Data Protection Regulation, the recordings of which continue to be available[2]. You may also find it useful to refer to our resources on safeguarding of vulnerable adults (where issues around data sharing are often relevant)[3] and case management[4] including examples of shared data systems (again where issues of data sharing are relevant).

Data sharing in meetings can cause anxiety for people whose organisations may not have clear policies and procedures to follow, particularly for case management type meetings where staff attending can be expected to talk about individual clients with staff from other organisations. People may be concerned about sharing too much information or not sharing enough information.

There are many different types of multi-agency meetings where information sharing about people using homelessness services may take place; these can sometimes be one-off meetings (sometimes referred to as case conferences) or regular meetings that form part of wider partnership working, such as Rough Sleeping Casework Panels or Complex Needs Panels. Other regular multi-agency forums may be community safety or crime and disorder meetings (which could include case level meetings such as MARAC or Joint Action Groups). These are generally intended to reduce crime and anti-social behaviour and protect vulnerable victims. Information may be shared verbally in these meetings but some data sharing by electronic means may also take place. Different types of homelessness services are involved in multi-agency forums.

This guidance explains some of the key terms and sets out some of the legal framework for the protection of personal data. It includes some examples of the sorts of situations in which personal information may be shared with other agencies. It also highlights some typical scenarios and suggests a framework that can be used to consider what information can be shared. Client consent to, and understanding of, information sharing should always be considered. General transparency and clarity of communication with clients about handling and sharing their data is very important to ensure their data rights are recognised. Do bear in mind though, in some situations, it is not necessary to have someone's consent to share information (or consent may not be the most appropriate legal basis for sharing).

Data protection and data sharing is a complex area and this should only be used as a very general guide (or even a discussion document) around data sharing in multi-agency meeting settings. **This is not a guide to data protection more generally**. It should supplement more detailed policies, procedures and training within your organisation. Most organisations will have at least one nominated person with responsibility for data protection who can provide further guidance on data sharing in multi-agency meetings.

Data sharing in multi-agency meetings is intended here to mean sharing of personal data with an external organisation or group of organisations. Your organisation may have a specific policy on data sharing (which will set out your organisation's approach and interpretation of some of the legal framework) or it may form part of your organisation's Data Protection Policy.

When personal data is regularly shared between organisations it is good practice to have data sharing agreements[5]. These are also referred to as Multi-Agency Data Sharing Protocols or Information Sharing Agreements. They usually set out the purpose of the data sharing, cover what happens to the data at each

[1] See https://www.homeless.org.uk/our-work/resources/effective-partnerships
[2] These are available to watch online, the third one maybe the most relevant to this guidance. See https://www.homeless.org.uk/introduction-to-gdpr
[3] See https://www.homeless.org.uk/our-work/resources/guidance-on-safeguarding-vulnerable-adults
[4] See https://www.homeless.org.uk/case-management
[5] See https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/

stage, set standards and help all the parties involved to be clear about their roles and responsibilities. If these are in place they will also provide further guidance to people taking part in meetings.

This guidance is based on the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR). Both are relevant to data sharing and came into force on 25th May 2018, together replacing the previous Data Protection Act 1998 (the provisions of the EU GDPR have been incorporated directly into UK law to become known as UK GDPR). They set out the framework for data protection law in the UK and the key principles, rights and obligations for most processing of personal data in the UK.

It is important to know that the UK GDPR and the DPA apply to all organisations and should be read together, however both recognise the different roles that public/statutory and non-statutory/voluntary organisations play. In some circumstance the rules affecting non-statutory organisations may differ from those applying to some statutory authorities such as local authorities and the police. One of the main areas where differences can occur is in establishing the appropriate 'lawful basis' for sharing data. There can also be differences between commissioned and non-commissioned services - where organisations are working with people experiencing homelessness under a contract with the local authority carrying out what might be termed 'public tasks' then that can be considered a lawful basis for sharing of data.

The guidance covers the whole of the United Kingdom however there are some variations for Wales, Scotland and Northern Ireland[6].

The Office of the Information Commissioner (ICO)

ICO is the UK's independent regulator for information rights including Data Protection with key responsibilities under the UK GDPR and DPA (and Freedom of Information Act 2000). They have a dedicated area of their website, the 'data sharing information hub'[7], which contains extensive information and guidance on data sharing (although it covers a vast range of situations including commercial/business sectors). A statutory Code of Practice on Data Sharing was produced by ICO and this came into force on 5th October 2021[8]. This is a comprehensive resource summarising the legal framework around data sharing including examples, checklists and templates. The code is mainly aimed at organisations that are data controllers sharing personal data. In particular, it is aimed at Data Protection Officers (DPOs) and other individuals within organisations who are responsible for data sharing matters. Below is a short extract from the Code:

When considering sharing data:

- you must comply with data protection law;
- we recommend that you assess the risks using a Data Protection Impact Assessment (DPIA); and
- it is good practice to have a data sharing agreement.

When sharing data, you must follow the key principles in data protection legislation:

- The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance.
- You must share personal data fairly and transparently.
- You must identify at least one lawful basis for sharing data before you start any sharing.
- You must process personal data securely, with appropriate organisational and technical measures in place.
- In your data sharing arrangement, you should have policies and procedures that allow data subjects to exercise their individual rights easily.

[6] See https://ico.org.uk/
[7] See https://ico.org.uk/for-organisations/data-sharing-information-hub/
[8] See https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

- You can share data in an emergency, as is necessary and proportionate. Examples of an emergency are the risk of serious harm to human life, or the immediate need to protect national security.

Data protection and data sharing – key terms

Understanding some of the key terminology can help in understanding approaches to data sharing and the legal framework. All of these terms are further explained by ICO in their data protection guidance for organisations[i].

Personal data
Personal data is any information related to a living individual that can be used to uniquely identify them including name, address, national insurance number or other official identification. Personal data includes items which can uniquely identify someone when combined, for example when a full name is combined with date and place of birth, or when a facial photograph is combined with other information. All personal data must be protected and can only be shared when conditions are met.

Special category data
Some personal data is defined as special category data, where it needs more protection as it is sensitive. Special category data is personal data which reveals someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used to identify a person) and data concerning their health, sex life and sexual orientation. Special category can only be shared if certain grounds apply.

Criminal Offence Data
The UK GDPR and DPA gives extra protection to 'personal data relating to criminal convictions and offences or related security measures'. This covers a wide range of information about criminal activity, allegations, investigations and proceedings.

Data processing
Almost anything an individual or organisation does with data/information on individuals is termed 'data processing' including collecting, recording, sharing, storing, using, analysing, combining, disclosing or deleting it.

Data Controller and Data Processor
An organisation that processes personal data will be defined in one of three roles:

- A data controller: if they collect or process personal data and make decisions on the purpose or means and outcome of the data processing.
- A data processor: if they follow the instructions of a controller regarding the processing of personal data.
- A joint data controller: if they are deciding the purposes and means of processing data jointly with another controller or other controllers – they are a joint controller.

An organisation can have multiple data sets and they can have different roles for each set of data.

Data Protection Officer (DPO)
A DPO is someone within an organisation who monitors internal compliance, informs and advises on data protection obligations and acts as a contact point for data subjects and the Information Commissioner's Office (ICO).

Lawful basis
An organisation must have a lawful basis (or reason) for processing personal data (including sharing it with another person or agency). This needs to be recorded as part of your documentation obligations and set

out clearly your privacy information for individuals. Lawful basis conditions for processing personal data are set out in Article 6 of the UK GDPR and you must be clear which of these is the correct one when you process personal data. These could include:

- Consent - where an individual has given clear consent for you to process their personal data for a specific purpose which includes sharing it with specific organisations. Consent must be informed and unambiguous. It must have been freely given and not be a condition of accessing your service. There must have been some positive action on the part of the client to constitute consent. This is often through signing of a consent form.
- Vital Interests - where personal data needs to be processed to protect someone's life, and the data subject is not capable of giving their consent such as sharing with a medical professional in the case of a medical emergency, or with the Police.
- Public Task - where personal data needs to be processed 'in the exercise of official authority'. This covers public functions and powers that are set out in law, or to perform a specific task in the public interest that is set out in law. This will mostly apply to public bodies but can also apply to a voluntary organisation where the LA had commissioned a service from them.
- Legitimate interest - where processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Any reliance on Legitimate Interests should be supported by a Legitimate Interests Assessment ("LIA"). This would not be appropriate for a statutory authority performing statutory duties.

For **special category data** additional conditions must be met for sharing. Explicit consent of the individual is one condition, but sharing special category data without consent could also be appropriate in situations relating to 'vital interest' where it is necessary to protect life or prevent death and it is not possible to obtain consent and also what are known as 'substantial public interest conditions' which could include safeguarding of children or individuals at risk. This is complex and use of these conditions may require specific policies to be in place - this an important area for thorough review as many types of multi-agency meetings are likely to cover sharing of special category data.

Privacy Notice
Privacy Notices are prepared by organisations that process personal data to explain to individuals the lawful basis they are using and more generally to explain how personal information is going to be used, who it will be shared with and why. Communicating clearly and transparently in ways which your clients can understand is important – it ensures you are complying with your client's rights to be informed. The Privacy Notice might also be referred as a data protection statement. Notices are often displayed on an organisation's website and examples from two voluntary sector homelessness services are listed in the further resources section (Connection at St Martins and Crisis).

Data Sharing Agreements
The Information Commissioner recommends that, where two or more organisations need to share personal data about their clients, an agreement should be drawn up and signed by all the organisations concerned. Such an agreement (often referred to as 'information sharing agreement') does not replace the organisations' responsibilities under the UK GDPR and the DPA, but it clarifies and sets out their responsibilities. Several examples of such documents can be obtained by running internet searches using key words. Some examples obtained in this way are listed in the further resources section (but note these are simply examples found through internet searches and are not presented here as good practice examples).

Data Protection Impact Assessments (DPIA)
A DPIA is a type of risk assessment to help you identify and minimise the data protection risks of a project or activity - you must do a DPIA for processing that is likely to result in a high risk to individuals and it's also good practice to do one for any other major project which requires the processing of personal data. It is

most likely to be undertaken by an expert or with advice from an organisation's data protection officer. An example template is provided by ICO and a link is included in the further resources section.

Individual information rights
Individuals who are data subjects have rights under the UK GDPR to be informed, to access their personal data, seek it to be deleted of suppressed or to challenge its accuracy. Individuals can make subject access requests (SAR's) of an organisation which processes personal data about them.

Preparing for multi-agency meetings

The following scenarios relate to multi-agency meeting settings, where an individual, team or organisation may be requested to share information with another organisation (or more than one organisation) about an individual who is experiencing homelessness or rough sleeping.

The scenarios developed for this guidance were written with voluntary sector organisations and teams in mind – they are designed to promote discussion within each organisation or agency, so that a position on sharing can be adopted in advance of the scenarios being encountered.

Obviously they are not an exhaustive list of all scenarios where individuals or teams may be asked to share data, and additional scenarios that staff members may encounter relevant to their roles should be considered and included in an organisation's internal training.

Across all scenarios we would suggest that the following key questions could be used to help you reach a position. These questions can act as a basic checklist for other situations too (although the ICO data sharing code also includes a checklist that could be used[9]):

- Is the data being shared personal data?
- Is it special category data?
- Who is the data controller?
- What is the purpose of data processing (in this case 'sharing')?
- What is the lawful basis for processing?
- If necessary, what conditions are there for sharing special category data?

In addition, we also recommend using the following questions to help align with good practice principles:

- Have you assessed the benefits and risks of data sharing using a Data Protection Impact Assessment (DPIA)[10] and considered having a data sharing agreement with the organisations involved?
- If there is a data sharing agreement when was this last reviewed to ensure it reflects changes in practice?
- Is it fair to share data in this way?
- Is the sharing necessary and proportionate to the issue you are addressing?
- What is the minimum data you can share to achieve the aim?
- Could the objective be achieved without sharing personal data, or by sharing less personal data?

[9] See https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/
[10] See https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/deciding-to-share-data/

- Where you are relying on consent – how have you ensured this is informed consent? How have you recorded this consent?
- What safeguards can you put in place to minimise the risks or potential adverse effects of the sharing? If sharing takes place electronically how secure is the data transfer?

Example Scenarios

Scenario 1

A local homelessness charity's outreach team have a policy of never asking the individuals they work with to complete assessments or paperwork, so they have not asked for consent from clients to share their personal data. They have regular positive contact with Person A who is sleeping rough and know a bit about A and her background.

They are invited to the local authority's multi-agency meeting on rough sleeping which brings together agencies to work collaboratively to provide advice and guidance, assessments, services, support and safeguarding for those who are rough sleeping, roofless or in unstable housing.

They are asked to share information about their work, and general information about any trends they are seeing in support needs. They are also asked to share A's name, age and nationality, and where they saw her sleeping rough on a particular night. They are unsure what information they can share

.

Using the questions:

Is it personal data?	Some is and some is not. Information relating to Person A is personal data – for example her full name or even first name if combined with age, nationality and rough sleeping location could uniquely identify the person. The person's nationality and even the fact they are sleeping rough may mean it is also special category data. Data is not personal data if it is anonymous information or if it is about general trends.
Who is the data controller?	Although we don't know if any data is recorded by the outreach service on the people they make contact with, we can assume they do know a name and would make some decisions about use of the information therefore this would suggest they are a data controller. They would have a good reason for collecting data and would need a privacy notice and some level of internal procedure and policy for how personal data is protected and when sharing may be appropriate.
What is the lawful basis for processing (sharing)?	In this case client consent does not appear to have been obtained so could not form the condition for lawful basis for sharing. The client would need to have consented to it being shared and made aware of the agencies it would be shared with and the reasons why. There could be other lawful bases which could include vital interest or, if the team are being funded under an agreement or contract working for the local authority, a lawful basis of 'public task'. There could be other grounds.
What is the purpose of processing (sharing)?	This depends on the purpose of the meeting. In this example the purpose of data processing may be: *'to provide advice and*

	guidance, assessments, services, support and safeguarding for those who are rough sleeping, roofless or in unstable housing'.
If necessary, what conditions are there for sharing special category data?	There is not likely to be any need to share special category data.

Conclusion
The team can share anonymised information that cannot be used to identify a living individual which would make the information sit outside the definition of personal data. Examples of data shared may include trends and unattributed anecdotes.

Consent has not been given by Person A and could not be used as a lawful basis for sharing personal information in the meeting. The team should not share any personal details about her unless operating under another lawful basis – which might be the case if the work they are doing is formally being undertaken on behalf of the local authority and where they are processing data under the lawful basis 'public task'. There could be other grounds too. In this situation the organisation's 'privacy notice' should cover this and it should have been brought to the attention of the individual.

If a specific intervention is being proposed to help meet Person A's needs it may be that the team can endorse or challenge it without sharing any personal data, for example by replying solely based on what is disclosed by others at the meeting.

Scenario 2

An Outreach Team has had a lot of contact with Person B. There are increasing concerns about B's health - he has bloody cuts and scratches on his body and appears underweight. His speech is rapid and the thoughts he expresses are jumbled and hard to follow. At times he can be verbally aggressive, shouting at the team to go away.

The team attend a multi-agency meeting with the purpose of working with other agencies to inform assessments and provide services to support the safety of individuals who are homeless in the local area. At the meeting there is a discussion about Person B's safety, and whether they would benefit from a mental health assessment. The team are asked to share what they know about B's history with housing and health services, and to describe what they have observed of his health needs.

Using the questions:

Is it personal data?	Yes: the information they hold relates specifically to the person and includes special category information about his health.
Who is the data controller?	If the team has collected and recorded the information they are being asked to share, and they make decisions about, and control, this data then they are the data controller. In this scenario we do not know what personal information they hold but it's likely to cover personal and special category data and we can assume they have some control over this data so they are likely to be the data controller.
What is the purpose of processing (sharing)?	It could be assumed from what is said that the purpose of processing would be to inform assessments and provide services and support to keep Person B safe.

What is the lawful basis for processing?	It is not clear if there is client consent – but most likely there is not because of the references to the client's request for the team to go away. It seems likely they would not be able to use client consent as the lawful basis for sharing. Vital interest could be a lawful basis in this case. If they were a commissioned service they may be able to use 'public task' as the lawful basis. There could be other grounds too.
If necessary, what conditions are there for sharing special category data?	Explicit consent could not be used in this case to share information about his health. However there are likely to be other conditions under the 'substantial public interest condition' if sharing might be necessary to safeguard an individual at risk. This would be best discussed with the data protection officer/lead within the organisation.

Conclusion

We do not know if there has been consent given by the individual for information to be shared but as he has told the team to go away and refused to engage, we can assume they were exercising their right to not consent to their data being shared. There may be grounds for sharing relating to for example vital interest or public task. There are some indications in this case that the client may be vulnerable and at risk of harm and there may be grounds for sharing the special category data in this case based on the substantial public interest conditions. This may be best discussed internally with the DPO or DP lead and subject to checking the organisation's privacy notice to decide if it would be reasonable and lawful to share information.

Scenario 3

A day centre is working with Person C, who has told them a lot about his past. C has previously given consent for his case to be discussed in the multi-agency homelessness meeting. More recently, he disclosed criminal convictions including sexual assault against a female.

The team are invited to a multi-agency meeting that meets to provide advice and guidance, assessments, services and support for those who are rough sleeping, roofless or in unstable housing.

Person C's case is discussed, and an accommodation offer is agreed, in a mixed-gender hostel by another provider. C's convictions have not been raised by anyone in the meeting. The team have concerns about risk to other residents if C moves into the hostel but are worried that they will breach data protection rules if they disclose what they have been told about his convictions.

Response:

Is it personal data?	Yes, if it uniquely identifies a living individual. Data about criminal convictions is not special category data. However, there are similar rules and safeguards for processing to deal with the particular risks associated with it, covered by UK GDPR and the DPA [11].
Who is the data controller?	It can be assumed that the day centre would collect and process data on people using their service and make decisions about how it is held and shared, and therefore the team would be the data controller.

[11] See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

What is the purpose of processing?	The purpose may be to provide advice and guidance, assessments, services and support for those who are rough sleeping, roofless or in unstable housing.
What is the lawful basis for processing?	We understand that the client has given consent to data being shared in the meeting so this is likely to be the lawful basis. It is important that the client is notified in a way they understand that information shared may include that related to the convictions they disclosed. Otherwise this could not be shared using this lawful basis ground. However there could be other lawful basis grounds that warrant sharing information.
If necessary, what conditions are there for sharing special category data?	In this specific instance there may be substantial public interest conditions relating to the safeguarding of other residents in the hostel that could be at risk of harm from C.

Conclusion

We do not know whether Person C consented for details of their past convictions to be shared in the multi-agency homelessness meeting. This is dependent on what person C was told at the time he gave his consent for his case to be discussed, and whether there were any limits on that consent in relation to particular subjects. If it is deemed that his consent covered the disclosure relating to criminal convictions, and consent was informed, unambiguous and affirmative (and could be evidenced as such) then the team may disclose what they were told. Other lawful basis grounds, including public task, could also apply if this is a commissioned service or legitimate interest. In this specific instance there may be substantial public interests conditions relating to the safeguarding of other residents in the hostel (that could be at risk of harm from C) to warrant the information being shared.

Alternatively it may be that the team obtains authority from their organisation's DPO (or DP lead) to discuss limited aspects of the situation with the chair of the multi-agency meeting and seek their advice on the protocol to be followed.

Scenario 4

A winter shelter are supporting Person D, who often sleeps rough, uses drugs and drinks heavily. He quite often appears to be under the influence of substances or alcohol, and does not remember people from one day to the next. He has given verbal consent for information sharing but the team are unsure that he really understood what was being asked.

They attend a multi-agency meeting where agencies work together to identify those experiencing multiple disadvantage and identify support that would help end their rough sleeping. At the meeting a new Housing First project is discussed. The team suggest this could be a great option for getting D off the streets. To start the referral process, they are asked to share information about his support needs and pattern of daily life, so that the Housing First team can make contact. The team are unsure what information is appropriate to share. They are particularly concerned that police attending the meeting might take action against D if they disclose his drug use.

Response:

Is it personal data?	Yes, it will uniquely identify a living individual
Who is the data controller?	It can be assumed that the service would collect and process data on people using their service and make decisions about how it is held and shared and therefore the team would be the data controller.

Homeless Link

What is the purpose of processing?	To work with those experiencing multiple disadvantage and identify services that would support them off the streets
What is the lawful basis for processing?	Consent might be the most likely lawful basis for sharing of personal data if this consent was given freely and was understood by the client. However there may well be other appropriate lawful basis such as vital interest, public task or legitimate interest.
If necessary, what conditions are there for sharing special category data?	If sensitive personal data is being shared (e.g. health) then explicit consent might be an appropriate condition. Without this there are unlikely to be other appropriate conditions for sharing.

Conclusion

In this scenario verbal consent has been given (we are not told what he consented to) but this is not likely be valid consent. The team felt that he was unsure what was being asked, and so consent could not be informed. It would not be inappropriate to proceed to share personal data in the meeting unless another lawful basis could be relied upon (which could be the case). It may be that explicit consent could be obtained after the meeting and information shared with the relevant organisations as a follow up.

On the specific point about sharing his *alleged*[12] drug use with the police, the protocol which governs the multi-agency meetings should be clear on how to deal with this. The meeting's purpose is to "work with those experiencing multiple disadvantage and identify services that would support them off the streets", however within the meeting protocol it needs to be clearly identified the remit of different agencies and what they do with the information, e.g. how the police act based on information shared in the meeting. The team should be aware of this prior to the meeting, however if staff are unsure about the meeting's purpose, or it comes to light during the meeting that data is being processed for a different purpose, they should consult with their organisation before sharing further data/information.

In this scenario the organisation's own privacy notice is particularly relevant. Their organisation may include something like "*There may be some circumstance in which we can share information without your specific consent, when it is reasonable and necessary to do so to fulfil our public tasks or it is otherwise in the substantial public interest to do so. We can share with: ….*").

[12] Drug used is *alleged* unless the team is properly qualified to diagnose this

Top Tips

The key tips below summarise what was covered in this document and in the scenarios:

All organisations should:

1. Have clear policies and procedures relating to data protection and data sharing.
2. Consider the need for Data Protection Impact Assessments to help capture risks and benefits of sharing personal data to inform their approach (and in some cases DPIA's may be legally required).
3. Ensure individuals and teams undergo training on general data protection principles, and the scenarios which may occur for them in relation to data sharing
4. Consider using multi-agency data sharing agreements which set out the roles and responsibilities of individual agencies when sharing personal data.
5. Ensure individuals and teams are clear on the purpose of any multi-agency meetings they attend, and consequently the purpose of data sharing
6. Ensure information sharing scenarios are considered ahead of meetings, so that attendees of multi-agency meetings come with knowledge of their own agency's protocols and approaches.
7. Ensure individuals and teams are empowered and encouraged to question the purpose of meetings and reasons for information sharing if not made clear beforehand. This allows individuals, teams and organisations to make decisions relating to how they participate in data sharing ahead of the meeting.

Staff should:

1. Be clear on the purpose of any multi-agency meetings they attend and consequently the purpose of data sharing.
2. Question the purpose of multi-agency meetings and data sharing if it is not made clear beforehand.
3. Be able to make decisions relating to how they participate in data sharing ahead of meetings, informed by their internal policies and procedures relating to data protection.
4. Know who in their organisation is the Data Protection Officer or other data protection specialist and how to contact them for advice and guidance on data sharing.

Further Resources

Homeless Link
Resources on effective partnership working and multi-agency meetings. https://www.homeless.org.uk/our-work/resources/effective-partnerships
Webinar recordings on GDPR https://www.homeless.org.uk/introduction-to-gdpr
Resources on safeguarding vulnerable adults https://www.homeless.org.uk/our-work/resources/guidance-on-safeguarding-vulnerable-adults
Guidance and resources on case management. https://www.homeless.org.uk/case-management

Examples of privacy notices
Connection at St Martin's https://www.connection-at-stmartins.org.uk/privacy-notice/
Crisis https://www.crisis.org.uk/get-help/sharing-your-personal-information-with-crisis/

Examples of multi-agency data sharing agreements
Norfolk Overarching protocol
www.norfolk.gov.uk/what-we-do-and-how-we-work/open-data-fois-and-data-protection/data-protection/data-sharing-agreements
A complex needs panel led by Ashfield BC
https://www.ashfield.gov.uk/media/hwkop2sq/complex-case-panel-policy.pdf
MARAC partnership in Bournemouth
https://www.bournemouth.gov.uk/communityliving/CrimeDisorder/DomesticAbuse/marac/marac-docs/personal-information-sharing-agreement.pdf

Information Commissioners Office
Data sharing information hub and Data Sharing Code https://ico.org.uk/for-organisations/data-sharing-information-hub/
ICO guidance for organisations on the UK GDPR and the DPA https://ico.org.uk/for-organisations/guide-to-data-protection/
Information on, and template for, DPIA's https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Appendix 1 – extra guidance when considering lawful basis for processing

Since so much of the data protection approach depends on the lawful basis for processing, the following might be helpful for agencies who are considering the basis for each of the sets of personal data that they process. However, obtaining specific advice from a data protection specialist or general advice from the ICO should be considered.

An organisation must be able to describe and justify its choice of the lawful basis for processing, from one of:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

In addition, if the personal data is defined as special category data (relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used to identify a person) and data concerning health, sex life and sexual orientation), then under Article 9 of the UK GDPR processing is prohibited unless one of the ten possible 'conditions for processing special category data' are met.
(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

The DPA supplements and tailors the UK GDPR conditions for processing special category data. Section 10 says that if you are relying on a UK GDPR condition which requires authorisation by law or a basis in law, you must meet one of the additional conditions in Schedule 1. Section 11(1) applies to the health or social care condition, and clarifies when the requirement for a professional obligation of secrecy will be met under UK law. Schedule 1 Part 1 contains the first four conditions, which give a specific basis in UK law for relying on specific Article 9 conditions:
1. employment, social security and social protection - Article 9(2)(b);
2. health or social care - Article 9(2)(h);
3. public health - Article 9(2)(i); and
4. archiving, research or statistics - Article 9(2)(j).

Schedule 1 Part 2 then specifies a further 23 potential 'substantial public interest' conditions for the purposes of Article 9(2)(g).

More information can be found on the ICO site here.

Special rules also apply to personal data concerning criminal allegations, proceedings or convictions and the ICO has more information here.

[i] See https://ico.org.uk/for-organisations/guide-to-data-protection/