Data Sharing Policy

1. Executive summary

1.1 South Lanarkshire Council, as a single tier local authority holds and uses information about people. There are times when there is a business need or a beneficial outcome for both the Council and the individual concerned (and the individual has consented for the Council to share the information) in relation to sharing that information with others. This sharing is governed by the Data Protection Act 1998 (the DPA).

1.2 The Council has put in place a series of policies, guidance and procedures, supplemented by additional Service/Resource based measures, in order to ensure compliance with the law. This policy has been prepared to assist in the decision making process regarding the sharing of information about people and the supporting measures that must be put in place.

1.3 Consequently, it is of more use to those employees of the Council who are engaged in the decision whether to set up and the setting up of data sharing arrangements. However, it will be supplemented by additional guidance/instructions for employees who are involved in the data sharing. In line with the Council's policies on data protection, the preparation and provision of this additional guidance or instructions will be the responsibility of the Resource who is undertaking the sharing of the information.

1.4 This policy sets down the matters that must be considered when setting up an arrangement to data share or providing information as a result of an ad hoc request for information.

1.5 Employees making decisions regarding the sharing of the information must have completed any supplementary training provisions put in place by the Council. For instance employees **must** have completed the following Learn Online Modules

- Introduction to the Data Protection Act
- How the Data Protection Act Works
- Subject Access Requests and
- Data Sharing.

Resources will be expected to be able to show that such employees have completed these online courses to the satisfaction of the Council by keeping appropriate training records that may require to be made available in relation to the review of any decisions to share personal data made on the behalf of that Resource.

2. Introduction

2.1 South Lanarkshire Council holds and uses a large amount of information about living identifiable individuals or information that when linked together says something about living identifiable individuals (personal data). There are times when Services within the Council pass or share that information both internally and externally with other public bodies, organisations, other Services within the Council or even individuals. This sharing is governed by the Data Protection Act 1998 (DPA) and non-compliance could have serious consequences for the Council including possible enforcement action or even a civil monetary penalty imposed by the Information Commissioner (currently up to a maximum of £500,000).

2.2 It could also have consequences in relation to the gathering of information by that public body etc if, for instance the information is being gathered in connection with a criminal prosecution or similar where the courts could rule the information gathered as being inadmissible (i.e. unable to be used).

2.3 In addition, the Information Commissioner (IC) has issued a Data Sharing Code of Practice[1] and the Council, as a data controller must have regard to the Code of Practice when sharing personal data. In his foreword to the Code of Practice, the Commissioner states that

"... under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors both public and private. But citizens' and consumers' rights under the Data Protection Act must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness"

2.4 Further, in its **Privacy Policy**, the Council has advised members of the public as follows

"*Who will we give someone's personal information to?*

From time to time, we will share someone's personal information with other bodies. Usually, we will only do this with his/her consent.

However, there may be times when we will share someone's information without consent, for example, with the police, the Health Service or other agencies. We will only share your personal information in compliance with the DPA".

2.5 Consequently, this Policy has been developed to try to ensure that the Council shares personal data in compliance with the 1998 Act, the IC's Code of Practice and also existing Council policies. It seeks to provide a framework of matters that Services must consider before sharing personal data, which will vary from situation to situation and so there can be no definitive guidelines as to when a Service should or should not share personal data. However, the decision as to whether to share personal data will be for that Service and it will be responsible for justifying its decision to share personal data and what to share.

[1] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

2.6 In line with the Council's policies and procedures in relation to data protection, this Policy sets out the overarching principles that must be followed when the Council is considering whether to share personal data. Executive Directors of each Resource will be responsible for the preparation, distribution and training of employees in relation to any Resource-based procedures implementing this Policy.

3. "Do and don'ts" summaries

3.1 It is vital that those employees who are considering whether
- the Council should share personal information and
- what arrangements need to be put in place

are fully aware of the Council's obligations under the DPA and so know and understand what the Council expects them to do when looking at issues around the sharing of personal information and so reaching decisions following this policy in full.

1.2 However, to assist employees this is a short list of "Do and Don't"s that you must take account of in making any decisions regarding data sharing. However, it is indicative only and should not be viewed as setting down all of the matters that you need to look at.

Do

1) Before considering whether to share personal data or to consider how to set up a system for data sharing, make sure that you understand the Council's obligations under the DPA as they relate to data sharing

2) Carry out a PIA in accordance with the required policy of the Council. This just doesn't look at security of the information but also whether you can actually share the information lawfully

3) After carrying out the PIA, assess what supporting measures need to be put in place. This could include considering and putting in place
   - how to advise the people concerned regarding the sharing of their information by providing a privacy notice
   - how to get the consent of the people concerned (where this is necessary) and measures that need to be put in place to do so and what to do if consent is withdrawn)
   - how to ensure that the sharing of the personal information is compliant with the DPA. You should use the Checklists contained in the Appendices to this policy – the answers to the questions should be in the PIA
   - whether there should be a data sharing agreement in place

4) If in doubt seek legal advice regarding the obligations of the DPA. The data sharing agreement must be prepared by Legal Services. However, this can only be done after the PIA has been carried out and the relevant Checklist considered.

5) Ensure that all data sharing arrangements are regularly reviewed for effectiveness and whether they still comply with the law.

Don't

1) Believe that there are times when the DPA does not apply to the sharing of personal data. This is not the case, even when sharing information in relation to a criminal investigation, the DPA will still apply.

2) Assume that there are times when a PIA is not required. Even if the trigger to share the personal information is a legal obligation on the Council, you must still carry out a PIA – the DPA still applies even if the sharing is compulsory.

3) Assume that the PIA is only about security. The purpose of the PIA is much wider and assists in the making of the decision as to whether the Council can actually share the information and what supporting measures, both technological and organisational (i.e. training of employees etc) must be put in place.

4) Assume that, because another Council or part of the Council shares the same information that it will be automatically ok to do so. The power and ability to share can depend upon circumstances and what arrangements have been put in place. You must carry out a PIA.

5) Assume that the recipient of the information is automatically entitled to get the information. This applies regardless of whether the recipient is the police or another part of the Council. The DPA applies to all sharing of personal data. The disclosure must be justified under the DPA. You will still have to put measures in place to take account of the rights of the people concerned

6) Think that the data sharing agreement allows you to share the personal information. If you have an agreement for a different purpose that covers the sharing of information with the same organisation etc, this does not give you the power to share any personal information for a different or additional purpose. You need to carry out the PIA and then see whether the existing agreement can be used with or without modification. If it cannot be then you will need a new agreement.

7) Think that the requirements to share information in terms of either a subject access request under the DPA or request for information under either the EI(S)Rs or FOISA replaces or regulates the power of the Council to share personal information.

4. Glossary of terms

4.1 Throughout this Policy, there are standard words and phrases used. These are based upon definitions contained within the Data Protection Act 1998. Unless they are defined in this Policy, they should be considered to have the same meanings as given to them in the Council's Guidance on the Glossary of Terms available on the intranet.

5. Sharing personal data

5.1 The sharing of personal data (which is sometimes referred to as "data sharing" or "information sharing") means, for the purpose of this Policy, the passing or sharing of personal data from a Service to another Service within the Council or with another body or organisation external to the Council.

Examples of data sharing given by the Information Commissioner are

- reciprocal exchange of personal data (a two way traffic of data)
- the Council or the Council with other organisations providing personal data to a third party or parties (a single way traffic of data) or allowing third parties access to Council records for their own purposes
- several organisations, including the Council, pooling personal data and making it available to each other
- several organisations, including the Council, pooling personal data and making it available to a third party or parties
- exceptional, one-off disclosures of data in unexpected or emergency situations; or
- different parts of the Council transferring personal data to each other (changing the purpose of the use of the information) or allowing other parts of the Council access to their records for their own purposes

However, for the purposes of this Policy, the information being shared must be personal data. Information which is not about one or more identifiable individuals or which does not or cannot be linked to other information and so identify anyone such as statistics is not covered by this Policy.

5.2 This Policy covers two main types of information sharing. They are

- "Systematic" data sharing and
- Ad hoc or ""one-off" data sharing

5.3 Systematic data sharing generally involves routine sharing (including pooling) of data sets between a Service and an external organisation or Services within the Council for an agreed purpose.

5.4 Ad hoc data sharing is where a Service decides or is asked to share data in situations that are not covered by any previous agreement or established rules and procedures.

6. Meeting the DPA

6.1 It is important to appreciate that it is for the Council as a provider of shared data to be able to justify its decision to provide the information. The purpose of the DPA is to provide for the regulation of the processing of personal data, including the obtaining, holding, use or disclosure of such information. It requires the Council to comply with the Data Protection Principles in relation to all personal data which it holds or uses (unless certain exemptions apply).

6.2 The first data protection principle says that the Council, when providing shared must meet one or more "conditions" in relation to the sharing of personal data (additional conditions must be met where it is sensitive personal data). One of these conditions is that the individual concerned has given consent for their personal data or sensitive personal data to be shared. If you are relying on consent then you must be aware that consent is to be viewed as being
"*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"[2]

6.3 However, you should not ask for consent or explicit consent (for sensitive personal data) where it is not needed to allow the Council to share the information. Sometimes, information will be being shared because to do so is necessary for a statutory function. In that case, it would be inappropriate to give a "choice" when in fact there is not one.

[2] European Directive 95/46/EC

The fact that consent is not needed is a separate matter from the requirement to provide a privacy notice.

6.4 Appendix 1 to this policy sets out the legislative framework for the Council to share personal data.

7. Facilitating data sharing

7.1 There are parts of the DPA that assist in relation to the sharing of information by allowing the Council to consider that it is not bound by certain obligations set down in particular parts of the DPA where to do so would be prejudicial to a recognised legitimate purpose.

7.2 The parts of the DPA that can prevent data sharing and so can be potentially relaxed are

- the first data protection principle (**except** the Council will always still need to be able to meet a condition set down in Schedule 2 (and if the information is sensitive personal data, a condition in Schedule 3) of the DPA to allow for the sharing of the information and
- the second, third, fourth and fifth data protection principles and
- sections 10 and 14(1) to (3) of the DPA.

These are cumulatively known as “the non-disclosure provisions”.

7.3 The exemption works by not obliging the Council to take account of any one or more of the non-disclosure provisions (each obligation needs to be considered in its own right) if by not doing so would prejudice certain important purposes (and only to that extent that the prejudice would be caused and no more).

Examples of these purposes are

- the sharing of information for the purposes of
  (a) the prevention and detection of crime (which needs to be a crime recognised by law)
  (b) the apprehension or prosecution of offenders and
  (c) the assessment or collection of any tax or any imposition of a similar nature **and**

  where not to disclose the information would be likely to prejudice those purposes (section 29(3) of the DPA)
- the sharing of the information is **necessary**
  (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
  (b) the purpose of obtaining legal advice

  or is otherwise necessary for the purposes of establishing, exercising or defending legal rights (section 35(2) of the DPA).

7.4 It is important to note that the extent to which the Council is not obliged to take account of one or more of the non-disclosure provisions needs to be considered on each and every occasion of data sharing and whether that non-disclosure provision still applies depends on the circumstances of each case. It would be possible for some of the non-disclosure provisions to apply where they do not cause any prejudice to a legitimate purpose.

7.5 Consequently, before the Council can take the view that it is no longer obliged to take account of one or more of the non-disclosure provisions, it must consider each transfer of personal data separately for each data subject. Therefore, the Council cannot

decide that it is not obliged to take account of the provisions in cases involving the sharing of personal data of multiple people or the sharing of personal data as part of a process involving systematic data sharing.

7.6 Further, it is for the requestor of the personal data to explain to the Council as to why it should decide that it is not obliged to take account of those provisions. For instance, the police could send the Council a notice in terms of section 29(3) asking for information about specified individuals in relation to a particular investigation. This notice sets out the information that is required by the Council to reach a view on whether to provide the information. As it will be for the Service who provides the information to justify doing so, it does not need to accede to the request unless it is satisfied that it can do so in compliance with the DPA. This is not the same as the body or organisation obtaining a warrant or a court order for the information.

7.7 However, it would be wrong to view the possible disapplication of one or more of the non-disclosure provisions as being a complete exemption from the obligations of the DPA even where the purpose of the sharing is connected to the investigation of criminal offences. The Council must still comply with the remaining provisions of the DPA even if the other person is investigating a criminal offence. There is little prospect of success in defending a decision by the Council to data share (even with another part of the Council) because the purpose may be related to investigation of alleged criminal activity. Trying to justify automatic ad hoc (using section 29(3)) or systematic data sharing purely because it relates to crime investigation may not be successful.

8. Data sharing for research/statistical purposes

8.1 Data sharing includes providing personal data and/or sensitive personal data to other parts of the Council or to bodies/organisations external to the Council for the purposes of carrying out research. In that case, the DPA allows for a minor relaxation of the obligations set down in it. In the case of research, which includes statistical purposes, the personal data and /or sensitive personal data cannot be used

- to support measures or decisions in respect of particular individuals, and
- in a way that substantial damage or substantial distress is, or is likely to be caused to any individual

8.2 Provided that the 2 conditions mentioned in paragraph 6.2 are met, the DPA disapplies the requirement on the person providing the information and/or carrying out the research to comply with the second and fifth data protection principles. However, all of the remaining data protection principles will apply even if the personal data and/or sensitive personal data are only being used for research purposes.

9. Privacy impact assessments

9.1 It is the policy of the Council that, regardless of the Service who is providing the personal data, before entering into any pre-planned data sharing arrangement (which is not a reaction to immediate events), you should carry out a Privacy Impact Assessment (a PIA). This helps to assess the benefits that information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

9.2 You should also assess potential harm to the Council's reputation which may arise if information is shared inappropriately or not shared when it should be. Further information regarding PIAs can be found on the Council's intranet.

10. Deciding to share - checklists

10.1 To help you in reaching a decision as to whether to share personal data, the Information Commissioner has prepared two checklists for you to use. These checklists are set out in Appendix 2 to this guidance. It is recommended that you always consult with them before reaching a view as to whether to share personal data as well as undertaking a PIA in relation to the proposal.

11. Data sharing agreements

11.1 All planned data sharing should be subject to either a data sharing agreement (which sets out the basis for sharing the information and how the personal data is to be shared) or an information sharing protocol which sets out how the personal data will be shared). This could be a separate agreement with or as part of a larger contract in relation to the provision of services by the recipient of the information.

11.2 Any Data Sharing Agreements must, at least, set out the following

- The purpose or purposes of the sharing
- The legal basis for sharing
- The potential recipients or types of recipient and the circumstances in which they will have access
- Whether the data is being shared through a data processor
- The data to be shared
- Data quality – accuracy, relevance, usability
- Data security
- Retention of shared data (including its eventual destruction etc)
- Individuals' rights – procedures for dealing with subject access requests, queries and complaints
- Review of effectiveness/termination of the data sharing agreement
- Any particular obligations on all parties to the agreement and
- Sanctions for failure to comply with the agreement or breaches by individual

11.3 Data Sharing Agreements will be prepared by Legal Services based upon the information provided to them by the Service concerned (the PIA will be of particular use in relation to helping to prepare the agreement).

12. Things to avoid

When sharing personal data, there are some practices that you should avoid. These practices could lead to regulatory action by the Information Commissioner against the Council as well as court actions. You must avoid

- Misleading individuals about whether the Council is sharing their information i.e. not telling them in case they object
- Misleading people regarding their right to withhold consent or to withdraw it at a future time (you should not imply that the data sharing is compulsory and that the data subject has to give consent etc)
- Sharing excessive or irrelevant information about people
- Sharing information when there is no need to do so
- Not taking reasonable steps to ensure that the information is accurate and up to date before you share it
- Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data
- Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal data

- Assuming that the recipient of the information has the automatic right to access the information i.e. the Council has no alternative but to provide the information because it is required by law to do so. This would only apply where the law has given the recipient the legal authority to demand the information and would be either set down in statute (or regulations or orders made under a statute) or as a result of a court order requiring the Council to provide the information. For instance even the police or someone investigating a criminal offence cannot require information from the Council without obtaining a warrant to do so. Even where there is a right to require information from the Council, it has to be satisfied that the right or power is being exercised properly.

13. Further information

For further advice or information on the data sharing policy contact:

Information Compliance Manager
Finance and Corporate Resource
Administration and Legal Services
Council HQ, Floor 13
Hamilton
ML3 0AA

Tel 0303 123 1015

Email: dp@southlanarkshire.gov.uk

If you need this information in another language or format, please contact us to discuss how we can best meet your needs.
Phone 0303 123 1015 or email equalities@southlanarkshire.gov.uk

Appendix 1– Legislative framework

There is no single source of law that regulates the powers of the Council to use and to share personal data. The collection, use and disclosure of personal data is governed by a number of different areas of law including

- The law that governs the actions of the Council (the Council's functions)
- The DPA
- The Human Rights Act 1998 and
- The common law duty of confidentiality.

1. Legislation covering the Council's actions

1.1 When deciding whether to data share, you need to start with ascertaining whether the Council has the power or is required to data share. The relevant legislation will probably be the provisions that set out the Council's functions, the things that it must do and the powers that the Council may use to meet its functions. Generally there are three ways that the Council could data share. These are

- **Express Obligation** – for instance, where the Council is legally obliged to share particular information with a named organisation. This will only arise in specific circumstances (and you need to be satisfied that the circumstances are actually subject to the obligation on the Council) but clearly if the Council is required to share the data, it must do so (provided that the legal duty applies)
- **Express powers** – for example the law says that the Council can share information for certain specified purposes (this is sometimes referred to as a "gateway" AND
- **Implied powers** – the Council does not have a specific power to share information but it is implied that it should do so in order to carry out a statutory function. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be related to and then check that the Council has the power to share the information.

1.2 If there are statutory restrictions on what information can be shared, then there is no power to do so.

1.3 However, even if there is a power to share information and the legislation itself does not restrict the sharing of the information, there are other statutes or laws that could make the sharing of the information unlawful.

2. The DPA

2.1 As mentioned, previously, the purpose of the DPA is to provide for the regulation of the processing of personal data, including the obtaining, holding, use or disclosure of such information. It requires the Council to comply with the Data Protection Principles in relation to all personal data which it holds or uses (unless certain exemptions apply).

2.2 If the sharing of the personal data does not comply with these principles (as they apply to it) then the sharing cannot take place (even if there is a specific statutory power to do so). For instance, the first data protection principle requires that the data subjects be given (or have access to) certain information prior to the collection of the personal data by the Council. This information includes to whom the personal data may be disclosed. A recent decision by the European Court of Justice has stated that, regardless of what the UK's domestic law says, this information must be given prior to the personal data being shared (where the sharing is pre-planned). The information is usually provided by means of a "privacy notice". Information regarding privacy notices can be found on the intranet.

3. The Human Rights Act 1998

3.1 The Council, as a public authority, must comply with the Human Rights Act 1998 (the HRA). Article 8 of the Convention of Fundamental Human Rights and freedoms gives respect to a person's right of privacy and this respect applies to the processing of personal data.

3.2 The Council can only interfere with the right to respect privacy under certain circumstances. However, it is likely that compliance with the DPA would also make the actions lawful under the HRA.

4. The Common Law Duty of Confidentiality

4.1 The general position is that if information is given to the Council by a third party (such as the data subject) where it is expected that a duty of confidentiality applies, that information cannot be disclosed without the information provider's consent.

4.2 This duty of confidentiality can only be overcome in particular circumstances such as where the disclosure is needed because it is necessary to safeguard the individual or others or is in the public interest (but only where that public interest outweighs the rights of the information provider) or the disclosure is required by a court order.

4.3 If you are in any doubt about whether there is a restriction on the Council to disclose/share the personal data then you should consult Legal Services before sharing the information.

Appendix 2 – Checklists for decisions re data sharing

Before asking anyone to share data with you or dealing with a request to share data from someone else, you need to make sure that you are clear about

- what the sharing is meant to achieve
- the potential risks, either to individuals or the Council or even just society more widely (with an aim to reducing these risks to an acceptable level – if not eliminating them all together) and
- the likely results of not sharing the data.

Based upon the guidance issued by the Information Commissioner in his Code of Practice, in order to do so, you must consider the following checklists depending upon whether you are considering ad hoc or systematic data sharing

Systematic data sharing

Is the Sharing Justified?
Key points to consider:

- ***What is the sharing meant to achieve?***
  You should have a clear objective or set of objectives. This will allow you to work out what data you need to share and who with.

- ***Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?***
  This assessment will be part of the considerations involved in conducting the Privacy Impact assessment for the sharing of the information. There is guidance in relation to PIAs on the intranet

- ***Is the sharing proportionate to the legitimate purpose that you are addressing?***
  You need to consider whether the sharing of the information needed in relation to meeting the issue and not excessive. Is it taking a sledgehammer to crack a nut? This would also be considered as part of the PIA.

- ***Can the objective be achieved without sharing personal data?***
  You need to consider whether the sharing is actually needed. This means that it must be more than just desirable but does not need to be the absolutely final option. You need to consider whether the objective be achieved without sharing the data or by the Council anonymising it before sharing it.? It is not appropriate to use personal data where the objective could be achieved by other means such as the use of anonymised personal data.

Does the Council have the power to share or is it obliged to do so?
Key points to consider:

- ***Does the Council have the power to share?***
  The Council must have the statutory power to share the information either expressly or impliedly or be required by law either by statute or court order to share the personal data.

- ***Is there anything that prevents the sharing?***
  Is there any legal impediment to sharing i.e. is it prohibited by either statute or common law (in relation to the duty of confidentiality.

If you decide to share
Key Points to consider:

- ***What information needs to be shared*?**
  You should only share as much information as is needed to achieve the objective(s). For instance, where a name and address is required but not a date of birth etc. you should restrict the information provided. Is the sharing of the personal data proportionate with the legitimate purpose for the sharing?

- ***How should it be shared?***
  You will need to consider the security of transmission of the data and set up appropriate measures etc to ensure security. It could be argued that the Council or the Service sharing the personal data is responsible for the safe transfer of the data and that it only becomes the responsibility of the recipient when the data is actually received by it.

- ***What you need to tell people about the data sharing of their personal data and how do you do so***
  You need to consider what should be stated in the privacy notice in relation to the sharing of the personal data and how should that notice be communicated. There is guidance on the intranet in relation to Privacy Notices.

- ***The management of the personal data after the sharing***
  You must consider whether the person or organisation with which you are sharing the personal data will process the personal data in a way that is compliant with the DPA. This does not mean that we are responsible for the actual use but must so far as possible ensure that the recipient meets their obligations. So you will need to ensure that the recipient will still respect the rights of the individuals to access their personal data and that the personal data will not be kept longer than is necessary for the recipient's legitimate purpose for obtaining the information.

Ad hoc data sharing

Is the Sharing Justified?
Key points to consider:

- ***Do you think you should share the information?***

- ***Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?***
  This assessment will be part of the considerations involved in conducting the Privacy Impact assessment for the sharing of the information. There is guidance in relation to PIAs on the intranet

- ***Do you have concerns that an individual is at risk of serious harm?***

- ***Do you need to consider whether any of the non-disclosure provisions need to be waived?***

Does the Council have the power to share or is it obliged to do so?
Key points to consider:

- ***Does the Council have the power to share?***
  The Council must have the statutory power to share the information either expressly or impliedly or be required by law either by statute or court order to share the personal data.

- ***Is there anything that prevents the sharing?***
  Is there any legal impediment to sharing i.e. is it prohibited by either statute or common law (in relation to the duty of confidentiality.

If you decide to share
Key Points to consider:

- ***What information needs to be shared*?**
  You should only share as much information as is needed to achieve the objective(s). For instance, where a name and address is required but not a date of birth etc. you should restrict the information provided. Is the sharing of the personal data proportionate with the legitimate purpose for the sharing? You must distinguish between personal data which is fact from that which is opinion.

- ***How should it be shared?***
  You will need to consider the security of transmission of the data and set up appropriate measures etc to ensure security. It could be argued that the Council or the Service sharing the personal data is responsible for the safe transfer of the data and that it only becomes the responsibility of the recipient when the data is actually received by it.

  You must be sure that you are sharing the information with the right person i.e. if the personal data needed in connection with the crime purposes in section 29 of the DPA the recipient must be a relevant investigatory body such as the police.

- ***Consider whether it is appropriate/safe to inform the individual that you have shared their information?***
  In terms of the first data protection principle you must give a privacy notice to each data subject advising him/her of the sharing of the information as part of one of the non-disclosure provisions. As mentioned earlier, you are not always obliged to provide a privacy notice where it would be prejudicial to recognised legitimate interests (see section 29 of the DPA). You will need to decide whether you are relying on the waiving of the non-disclosure provision regarding a privacy notice so that purpose of the information being requested is not prejudiced. The Council's standard style of Section 29(3) Notice asks whether the non-disclosure provision about a privacy notice should be waived. It is for the requestor to satisfy the Council that this is the case/ If not satisfied, you will need to provide a privacy notice to the person concerned before sharing the personal data.

Record your decision:
Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share the information you should record
- ***What information was shared and for what purpose***
- ***Who it was shared with***

- ***When it was shared***
- ***Your justification for sharing and***
- ***Whether the information was shared with or without consent***