Item 14

Renfrewshire Council

To: Finance & Resources Policy Board

On: 26 August 2015

Report by: Director of Finance & Resources

Heading: Data Sharing Code

---

1. **Summary**

1.1 'Data Sharing' is regulated by the Data Protection Act 1998 and refers to the disclosure of data to a third party organisation(s) or the sharing of data between different departments of the Council. The Council needs to routinely share data for a number of different reasons. As such, in 2012, the Council developed a data sharing code based on the guidance of the Information Commissioner's Office. This was approved by the General Management and Finance Policy Board on 29 August 2012 and is now due for a three yearly review.

1.2 The proposed revisals to the Data Sharing Code are minor and are attached as Appendix 1. This been updated to include more detail on the application of Privacy Impact Assessments ("PIAs"), an Appendix on Data Standards and the current arrangements for information governance within the Council.

---

2. **Recommendations**

2.1 That the Board approve the revised Data Sharing Code and agree that this is reviewed on at least a three yearly basis by the Information Governance team and approved by the Council's Data Protection Working Group. An earlier review will be carried out should any legislative change or new ICO guidance require this.

3. Background

3.1 This code explains how the Data Protection Act 1998 (DPA) applies to the sharing of personal data. It also provides good practice advice that will be relevant to all Council officers who share personal data.

3.2 Adopting the good practice recommendations in the code will help Council officers to collect and share personal data in a way that is fair, transparent and in line with the legislation and the rights and expectations of the public. The code will help Council officers to identify the considerations when deciding whether to share personal data. It is intended to give officers confidence to share personal data when it is appropriate to do so, but also provides a clear outline of when it is not acceptable to share data.

Implications of the Report

1. **Financial** – none.
2. **HR & Organisational Development** - – none.
3. **Community Planning –** none.
4. **Legal** – the revised Data Sharing Code will ensure the Council continues to comply with the legislative requirements of the Data Protection Act 1998 in relation to data sharing.
5. **Property/Assets –** none.
6. **Information Technology** - – none.
7. **Equality & Human Rights** -The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report. If required following implementation, the actual impact of the recommendations will be reviewed and monitored, and the results of that assessment will be published on the Council's website.
8. **Health & Safety –** none.
9. **Procurement –** none.
10. **Risk –** none.
11. **Privacy Impact –** none.

List of Background Papers

N/A

Author: Allison Black, Managing Solicitor (Information Governance)
Alison.black@renfrewshire.gcsx.gov.uk
0141 618 7175

Renfrewshire Council

Data Sharing Code

Version	Date	Author	Reason for Issue/Change
1	August 2012	Allison Black, Assistant Managing Solicitor	
2	May 2015	Allison Black	Three-yearly update

Document History

Document Review and Approval

Name	Action	Date	Communication
Mary K Little, information Security Officer	Consulted	03/02/15	Email
Joseph Bartoletti, Records Manager	Consulted	03/02/15	Email
Heather Semple, Solicitor (Information Governance)	Consulted	03/02/15	Email
Data Protection Working Group	Consulted	May 2015	Email
Information Management Governance Group	Consulted	May 2015	Email

Related Documents

Ref	Document Name/ Version	Document Location
1		
2		
3		

Title	Data Sharing Code
Author	Allison Black
Issue Date	
Subject	Data Protection
Description	
Version	
Source	
Updating Frequency	Three Yearly
Right	
Category	
Identifier	

1. Introduction

1.1 The Council must collect and share Personal Data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.

1.2 The Data Protection Act 1998 ("DPA") contains the rules on how Personal Data must be handled. Data sharing across and between organisations can result in the provision of a more efficient service to the public. It is often of benefit to the Council to data match, on both a cross-departmental and cross-agency basis, for a variety of purposes including debt recovery, keeping information up to date, protection of individuals or simply just to ensure that the correct services are being delivered to those who need them. It is essential, however, that any data sharing complies with the DPA.

1.3 The Council is also bound by the Human Rights Act 1998 and is a signatory to the Information Commissioner's ("ICO's") Information Promise, which reassures the public that their personal information will be carefully handled.

1.4 Using data for more efficient service delivery is clearly of benefit to the public. However, the focus of the DPA is on individual rights. Therefore, although many people may expect their information to be shared, in the interests of efficiency, people also expect organisations, such as the Council, who are entrusted with their personal information, to keep this safe and secure. Individuals also expect a level of choice over the use of their data. Respect for privacy does not necessarily mean that there should be unnecessary restrictions imposed on the use of information. It does, however, require transparency. In the interests of openness, individuals should be made aware of how their information will be used if it is appropriate to do so.

1.5. Although a breach of the DPA is a very serious matter, it is important that data protection is not seen as an obstacle to effective information sharing, especially when this is necessary to protect individuals. Misunderstanding of what information can and cannot be shared can disadvantage service users. Reluctance to share information can be as harmful as carelessness. However, individuals need to be confident that the Council is handling their information properly.

1.6 This Code is based on the ICO's Data Sharing Code of Practice, which was prepared and published under section 52 of the DPA. Although the ICO Code, as a statutory Code, which has been approved by the Secretary of State and laid before Parliament, does not impose additional legal obligations, compliance with this is the best way of demonstrating compliance with the DPA when sharing personal information. This is because the Information Commissioner, courts and tribunals must take into account any part of the Code which appears relevant in dealing with data protection cases.

1.7 All employees and Elected Members have a responsibility to ensure that they understand when it is appropriate to share Personal Data. This Code will help them to collect and share Personal Data in a way that is fair, transparent and in line with the expectations of the public, It will identify the issues which staff need to consider when deciding whether to share Personal Data, give them the confidence to share, where appropriate, and a clear idea of when it is not acceptable to share.

1.8 If you are in any doubt about sharing information, you should seek further help, advice, support and/ or assistance from your the Information Governance Team.

2. Scope

This Code applies to all Services, employees and Elected Members of Renfrewshire Council and takes account of the provisions of the ICO Data Sharing Code of Practice. It applies only to the sharing of Personal Data. Personal Data is information which can be used, either alone or, with other information held, to identify a living individual.

3. What is Data Sharing?

'Data sharing' is the disclosure of data to a third party organisation(s) or the sharing of data between different departments of an organisation. Data sharing can take the form of:-

- a reciprocal exchange of data
- provision of data to a third party
- the pooling of information by several organisations and making it available to each other or other organisations
- exceptional, one-off disclosures of data in unexpected or emergency situations
- sharing between different departments of the same organisation.

4 Types of Data Sharing

4.1 Any sharing of information should be

- Relevant;
- Necessary;
- Legitimate;
- Appropriate; and
- Proportionate

4.2 This Code covers two different types of data sharing:-

- **Systematic**: routine data sharing where the same information is shared between the same organisations for an established purpose; and
- **Exceptional**: one-off decisions to share data for a range of purposes.

Each type of data sharing should be approached differently. Some of the considerations that apply to systematic, routine data sharing are not relevant to one-off decisions to share data. A checklist for both is annexed at Appendix 1.

4.3 Systematic Data Sharing

Public sector organisations need to share routinely share data for a number of different reasons. It is good practice for such arrangements to be formalised by Information Sharing Protocols ("ISPs"). A checklist for information which should be covered in ISPs is annexed at Appendix 2.

4.4 One-Off Data Sharing

The Council is regularly approached, on a case by case basis, to share data. In some cases, other organisations will have statutory powers to access information, in which case they should be able to confirm this authority. Where the requester has no such powers, the conditions in Schedule 2 to the DPA (and Schedule 3, when dealing with Sensitive Personal Data) may allow for the sharing. For example, if there are concerns that someone is at risk of serious harm, the information can be shared on the basis that it is 'necessary to protect vital interests'. Consideration should also be given to the exemptions in the DPA which recognise that, in some cases, Personal Data may need to be shared.

For example, there is an exemption which gives the Council the discretion to share with the Police, or other organisations, if failure to do so would be prejudicial to the prevention or detection of crime or the apprehension or prosecution of offenders. If approached by the Police, or other organisations, for Personal Data, for this reason, a 'section 29(3)' certificate must be obtained from them. Further information on exemptions can be obtained from the Information Governance Team.

4.5 Data Processors

The DPA draws a distinction between data sharing between the Council and another data controller and providing another party with data simply to process on the Council's behalf. If someone, other than an employee of the Council, is processing personal information on the Council's behalf, for example, a contractor, the Council, as data controller, is obliged under the DPA to have a written agreement or contractual obligation. This is to ensure that the data processor will comply with the seventh principle by keeping that information secure.

In other words, there should be a written agreement that appropriate technical and organisational measures will be taken by the contractor to keep the Personal Data

secure. This is because a data processor does not have any data protection responsibilities of its own. They are only imposed through its contract with the Council and the Council, as data controller, has responsibility for the data. Advice can be obtained on data processor agreements, at any time, from the Information Governance Team.

4.6 Inter-departmental Sharing

The data protection principles apply to data sharing between Council departments. Although the Council is a single data controller, the second principle that data should be used only for one or more specified purposes is particularly relevant to this type of data sharing and consideration will always need to be given as to whether this is fair and lawful.

5. When Can Data Be Shared?

1. When there is a legal power or duty to do this and
2. When it complies with the DPA

5.1 Legal Powers

There are both real and perceived barriers to data sharing. Before the Council can data share, it needs a legal power to do so. Where there is no power to share particular information, this will present a real barrier to information sharing.

Councils can only do what they are required or authorised to do by statute. If a local authority has no power to do something but proceeds to do it, in excess of its powers, this will be 'ultra vires' (i.e. outwith the Council's legal powers) and, as such, legally void.

Data protection compliance can only be considered once 'vires' (a legal power) is established.

The Council has:-

- Express duties – occasionally, the Council will be legally obliged to share information with certain organisations e.g. DWP.
- Express powers – sometimes there is a specific legislative provision which allows for specific information sharing, often referred to as a "gateway."
- Implied powers – the Council has many powers to do things which are reasonably incidental to those which are expressly permitted.

If the Council does not have the legal power to conduct a particular data sharing exercise, even compliance with the DPA will not make this lawful. For example, the provisions of the Local Government Finance Act 1992 often prevent use of council tax data for non council tax purposes. In such cases, even where the Council can

comply with the DPA, it would still be unlawful to share this data. However, if the proposed data sharing is covered by a legal power, the rules in the DPA must then be considered.

5.2 Data Protection Compliance

5.2.1 Fair and Lawful Processing

The DPA is based on eight data protection principles, which contain the rules on how personal information should be handled. The data protection principles are annexed at Appendix 3.

The first two principles are generally the main considerations when data sharing. The first principle is that data must be processed fairly and lawfully. The second principle states that Personal Data shall be processed only for one or more specified purpose(s). Fair processing simply means that an individual should know what uses will be made of his/her personal information. Respect for privacy does not necessarily mean that there should be unnecessary restrictions imposed on the use of data. It does, however, require transparency.

In the interests of openness, individuals should be made aware of how their data will be used This is why the Council has a privacy policy on its website, advising people of how their data will be handled and why any Council form, which collects Personal Data has a data protection declaration, advising people of what will be done with their data, by whom.

Lawful processing is more complex. The DPA lists a number of conditions for lawful processing of Personal Data and there are some stricter rules which must be followed for Sensitive Personal Data. Sensitive Personal Data is information relating to racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, health, sexual life, commission or alleged commission of any offence or court proceedings, disposal or sentence. Lawful processing of Personal Data requires that at least one of the conditions in Schedule 2 to the DPA must be met, whereas a further condition from Schedule 3 must also be fulfilled when processing sensitive Personal Data. These conditions are listed in Appendix 4.

Although consent is not the only justification for processing of Personal Data, it is generally the only condition which is applicable to wholesale data sharing. This is largely due to the fact that the other conditions can only be applied to fairly specific circumstances. For example, it would be difficult to justify data sharing as being necessary to protect the vital interests of the data subject when an extensive data sharing exercise is being carried out, regardless of whether this is to simply increase efficiency or protect the public purse. Similarly although the Act allows data controllers to pursue legitimate interests, the proviso to this is that this must not prejudice the rights of data

subjects. As a result, there will usually be a requirement for consent for large scale data sharing exercises.

This is why it is important that all Council forms which collect Personal Data contain a declaration advising what use(s) will be made of Personal Data. Signature of the form ensures that the processing is both fair and lawful, as this will provide consent to the processing described. This will also meet the requirements of the second condition that Personal Data is being used for one or more specified purpose(s). A sample declaration is provided at Appendix 5. Although there is no requirement for consent to be in writing, there must be some form of record kept that service users have consented to what is being done with their data.

5.2.2 Privacy Notices

Privacy notices are an important way of ensuring that processing is fair and should be provided when an individual's data is first collected. This is particularly important when the Council wishes to use data in a way which is not obvious, as this needs to be made clear to people. As well as the generic privacy notice on the Council's website, each Council form, which collects Personal Data should contain the data protection declaration, attached at Appendix 5. Declarations for use by Customer Service Unit staff are also attached. In a data sharing context, any privacy notice should be clear on:-

- Who the Council is
- What Personal Data will be shared
- Why Personal Data will be shared
- Who it will be shared with

5.3. The Human Rights Act 1998

The Human Rights Act 1998 ("HRA"), also needs to be considered before data sharing. The Act incorporates most of the Articles of the European Convention on Human Rights (ECHR) into UK law. Art 8 ECHR affords everyone the right to respect for private and family life, including home and correspondence. Although this right is not absolute, any interference must be justified on the basis that it is lawful, necessary to pursue a legitimate aim and proportionate i.e. the interference should not be greater than is necessary to achieve the aim. In other words, "a sledgehammer should not be used to crack a nut." Although compliance with the DPA will mean that an interference is lawful, the Council also needs to consider whether any data matching exercise is necessary in the public interest, or whether the same ends can be achieved by a less intrusive means before an interference with Art 8 can be justified.

6. Key Considerations

When deciding whether to share data, the potential risks and benefits to either individuals or society, must be considered. It is also important to consider the risks of not sharing the information.

Local authorities need to share Personal Data for a variety of purposes. It is often difficult to reconcile privacy issues with data sharing for the common good and the DPA can appear to be an obstacle to effective information sharing. Anecdotal evidence indicates that the public perception is that increased efficiency and more joined-up service delivery within the public sector is desirable, yet at the same time, the public do not want increased sharing of their personal details.

Failure to share information can, in some cases, be more harmful than carelessness. Data protection is not always a barrier to information sharing which is necessary and in some cases, public sector organisations actually need to consider the risks of not sharing information. Data protection is about information rights and the protection of people's information. Although there are inevitable tensions between information sharing and data protection, the DPA should not be regarded as conflicting with individual rights.

The following should be considered:-

- What is the sharing meant to achieve?
- What information needs to be shared? – This should be no more than is necessary. Never share irrelevant or excessive information about people.
- Who needs access to this? Is there a 'need to know'? –If not, the information should not be shared.
- When should it be shared?
- How should it be shared? – Any data shared must be securely transmitted. For example, Sensitive Personal Data should never be faxed to an office number or transmitted via insecure email. Using incompatible information systems could result in loss, corruption or degradation of data.
- How can it be checked whether the sharing is achieving its objectives?
- What risk does the data sharing pose?
- Could the same objective still be achieved without sharing or by anonymising the data? –If so, the sharing may breach the HRA, as well as the DPA, as it will be disproportionate.
- Does the Council's annual notification to the ICO need to be updated to cover the sharing?
- Will any of the Personal Data be transferred outwith the European Economic Area? – If so, further advice on this should be sought from the Council's Information Security Officer.

7. Security

The seventh data protection principle obliges the Council to have appropriate technical and organisational measures in place to protect the security of data being shared. Consideration should always be given to any security risk in sharing the data, the impact of sharing the data on both the individual and the Council in cost, reputational damage or lack of public confidence. Personal Data should only ever be accessed and / or shared when there is a legitimate business reason. It is important to be clear on who will have access to the data and what it will be used for in the recipient organisation. Data must be protected in accordance with the sensitivity of the data. Advice on the handling of data and the secure transmission can be obtained from the Council's Information Security Officer.

8. Individual Rights

Individuals have a right under the DPA to object when the use of their Personal Data is causing them substantial, unwarranted damage and distress. The objection can be to the use of the information or to the mere fact that the Council is holding their Personal Data at all. The Council is obliged to respond, within 21 days, to individuals who object in writing. However, it does not need to comply with the request unless there is damage or distress and this is substantial and unwarranted. Clear reasons should be provided if the objection is considered to be unwarranted. If the individual's request is complied with, the steps taken and timescales for this should be explained.

The best way of avoiding objections is to provide individuals with clear information about the basis on which the Personal Data is being shared and how it will be used.

9. Notification

The Council is obliged to annually notify the ICO of the individuals or organisations to whom it intends to disclose Personal Data. Consideration should be given as to whether the Council's notification needs to be updated to reflect any new data sharing arrangements. Any updates should be provided to the Records Manager, who is responsible for maintaining the Council's notification with the ICO.

10. Privacy Impact Assessments

10.1 Privacy Impact Assessment (PIA) is a process which enables organisations to address the potential privacy risk and impact from the collection, use and disclosure of personal information as a result of new initiatives. The purpose of the PIA is to ensure measures are in place to make sure data protection compliance and privacy concerns are addressed.

10.2 A PIA should be considered for any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals. It is designed to identify any privacy risks and ensure that those risks are minimised while still allowing the aims of the project to be met. A PIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

Examples of where a PIA would be helpful:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of the Council.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.

10.3 Carrying out a PIA will assist with considering whether data should be shared and will help assess any potentially negative impact on people's privacy. Further information on PIAs can be obtained from the Information Governance Team or the Information Governance pages on Renfo.

11. ICO Powers

The ICO has a number of enforcement powers, including, since April 2010, the power to impose a monetary penalty of up to £500,000 for the most serious breaches of the DPA. Individuals have the right to seek an assessment from the ICO if they feel that their rights under the DPA have been breached and can sue the Council for damage and distress.

12. Review

This Code will be reviewed on at least a three yearly basis by the Information Governance team and approved by IMGG. An earlier review will be carried out should any legislative change or new ICO guidance require this.

Appendix 1

Checklists for Data Sharing

Systematic Data Sharing

1. Is there a legal power/duty to share?
2. What is the sharing meant to achieve?
3. Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
4. Can the same objective be achieved without sharing personal details?
5. Is there a less intrusive way of achieving that objective?
6. If Personal Data does need to be shared, how much is there a need for the requester to know?

One Off Requests

1. Do you think you should share?
2. Have you assessed the benefits/risks?
3. Do you have concerns that an individual is at serious risk of harm?
4. Is there a legal obligation to share?
5. Do you need to consider an exemption in the DPA to share?
6. What information do you need to share? – Only share what is necessary and distinguish fact from opinion.
7. How should the information be shared? – Information must be shared securely.
8. Is it appropriate/safe to inform the individual that you have shared their information?
9. Record your decision and your reason-whether or not you shared the information.

Appendix 2

ISP Checklist

What should an Information Sharing Protocol ("ISP") address?

In the simplest of terms, a Protocol should include the following:

Why? Who? What? How? When? On what basis? With Whom?

Why? Outline the purpose of the ISP and its objectives.

Who? Identify the organisations that will be involved in the sharing. It is important however that as well as clarifying inter-agency data sharing procedures, protocols provide at least broad guidance to staff on how subject access requests ("SARs") by users should be handled. Once Personal Data comes into the possession of another data controller, that data controller becomes bound by the provisions of DPA, including the subject access rights.

What? The ISP should explain the types of data it is intended to share.

How? Inter-agency data sharing can only be made easier if the procedures detailed in the protocol are clear. It is therefore essential that certain key issues are addressed, such as:-

- Management of the protocols.
- Training needs
- Breaches –ISPs need to be monitored and kept under review.
- Transfer of information, shared information standards and security procedures - all parties should be clear on how information will be transferred between them and what security measures are required.

When? Clauses on general principles and specific purposes for which information will be shared will assist those involved in the implementation of the protocols.

On What Basis? Outline any legal power or duty. If consent is the basis, issues around sharing withholding or retraction of consent should be covered and a model consent form.

With Whom? The parties to the protocol will be clearly outlined.

Appendix 3

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, shall not be processed unless at least one condition from Schedule 2 is met and, in the case of Sensitive Personal Data, at least one of the Schedule 3 conditions is also met.

2. Personal Data shall only be obtained for one or more specified and lawful purpose(s).

3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal Data shall be accurate and, where necessary, kept up to date.

5. Personal Data shall not be kept for longer than is necessary.

6. Personal Data shall be processed in accordance with the rights of the data subject.

7. Appropriate technical and organisational measures shall be taken to prevent against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal Data shall not be transferred to a country outwith the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data.

Appendix 4

Conditions for lawful processing - Data Protection Act

Schedule 2

Personal Data can only be lawfully processed if ONE of the Schedule 2 conditions is met:-

The data subject has consented to the processing

The processing is necessary for compliance with a legal obligation

The processing is necessary to protect the vital interests of the data subject

The processing is necessary for the performance of a contract to which the data subject is a party.

The processing is necessary for the administration of justice

The processing is necessary to pursue a legitimate interest but this must not prejudice the rights and freedoms or legitimate interests of the data subject.

Schedule 3

Sensitive Personal Data may only be processed when at least one condition from Schedule 2 is met and one of the following is also met:-

The data subject has given explicit consent to the processing

The processing is necessary in terms of employment law

The processing is necessary to protect the vital interests of the data subject or any other person when consent cannot be obtained

The information has already been made public as a result of steps deliberately taken by the data subject

The processing is necessary for legal proceedings

The processing is necessary for the administration of justice or for the exercise of any functions conferred by enactment.

Appendix 5

Declarations

Suggested wording for Customer Service Centre Staff and frontline staff taking personal details

> "May I take a few personal details? These may be shared with other Council departments and other public sector organisations, as appropriate, to improve the service we provide to you, check accuracy, protect public funds and to prevent or detect crime."

Suggested wording for Council forms

> This wording should be adapted, as necessary, by Services, to reflect the processing which will be carried out. Very little detail is required if no data sharing is envisaged.
> It should be noted that whilst the declaration itself should be placed above the place for signature on the form, without providing an opportunity to opt out, people must be able to opt-out of any additional marketing element (and actually opt in if this marketing will be done by electronic means, such as email, text or automated marketing calls) e.g. if the Council wishes to contact them in future about other events/services which may be of use to them, or pass their details to other organisations for marketing purposes.
>
> The Data Protection Act 1998
>
> The information you have given will be used for the purposes of [outline all of the purposes for which the data will be used]. The Council may check your details with other information held and may share these with other Council departments and [outline any other relevant agencies to whom a disclosure will be made and specify if for any different purposes] to check the accuracy of the information; to prevent or detect fraud or crime or to protect public funds. [any additional purposes should be highlighted and inapplicable purposes should be deleted accordingly.]"
>
> If necessary, something along the following lines should be added on a separate line and a tick box should be inserted:-
>
> "The Council may send you details of similar events/services [any other uses should be detailed] which may be of interest to you. If you do not wish to receive this information please indicate this."
>
> or if creating a database for "marketing"
>
> "The Council will add your details to a database which will be used by the Council [and our community planning partners? Any other parties should be

listed] to send you details of [similar events/services?] which may interest you. Please indicate if you do not wish to have your details added to the database."

People must, however, be asked to opt-in when the consent is being obtained to market by electronic means. In other words, they should indicate if they **do** wish to be contacted.

Appendix 6 – Data Standards

It is important to have procedures in place to maintain the quality of the Personal Data held, especially when you intend to share data. When you are planning to share data with another organisation, you need to consider all the data quality implications.

When sharing information, you should consider the following issues:

- Be clear with individuals if you intend to share their information.
- Do not share excessive or irrelevant information about people.
- Make sure that the format of the data you share is compatible with the systems used by both organisations
- Check that the information you are sharing is accurate before you share it
- Make sure appropriate security measures are in place
- Agree common retention periods and deletion arrangements for the data you send and receive