WEST LOTHIAN COUNCIL

DATA SHARING CODE OF PRACTICE

Version 1.1

September 2019

Data Label: Public

Document Control Sheet

DATA LABEL: Internal

AUTHOR: David Robertson, Information Team Manager (Social Policy)

DOCUMENT TITLE: West Lothian Data Sharing Code of Practice

Review/Approval History

Date	Name	Position	Version Approved
03/02/2011	Julie Whitelaw	Chief Solicitor	1.0
03/02/2011	Roberto Riaviz	Information Strategy & Security Manager	1.0
10/11/2011	Information Management Working Group	N/A	1.0
18/07/2012	ICT Programme Board	N/A	1.0

Change Record Table

Date	Author	Version	Status	Reason
16/12/2010	David Robertson	0.1	Draft	Initial draft for review
03/02/2011	David Robertson	1.0	Final	Agreed Version
25/09/2019	Carol Dunn	1.1	Final	Minor updates

Status Description:

Draft - These are documents for review and liable to significant change.
Final - The document is complete and is not expected to change significantly. All changes will be listed in the change record table.

CONTENTS

FOREWARD

The purpose of this document is to give a local, West Lothian specific version and interpretation of the Code of Practice issued by the Information Commissioners Office (ICO) on data sharing. Where appropriate, links to existing supportive documentation such as policies, examples and protocols have been embedded within this code of practice to assist with the practical application of the procedures recorded herein. This data sharing code of practice should be referenced in all and any instances of information and data sharing with West Lothian Council and Community Health and Care Partnership.

What do we mean by 'data sharing' in West Lothian?

This code of practice is about the sharing of personal data. By "data sharing" we mean the disclosure of personal data from one or more organisations or service areas to a third party service area, organisation or organisations. Data sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations/service areas providing data to a third party or parties;
- several organisations/service areas pooling information and making it available to each other;
- several organisations/service areas pooling information and making it available to a third party or parties;
- different parts of an organisation making data available to each other; or
- exceptional, one-off disclosures of data in unexpected or emergency situations.

Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither Data Protection law, nor this code of practice, apply to that type of sharing.

The code covers the two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

Different approaches apply to these two types of data sharing and the code of practice reflects this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing. It should also be noted that this code of practice may be considered helpful when addressing issues around non-recorded data sharing, such as conversations relating to personal information of clients in a shared environment.

Within West Lothian all uses of information must follow the guidelines as indicated within the Information Security Guidance.

About this code

This code explains how the Data Protection law (the General Data Protection Regulations 2016 and Data Protection Act 2018) applies to the sharing of personal data. It also provides good practice advice that will be relevant to all service areas that share personal data.

The code covers activities such as:

- sharing client assessments, alert, planning or chronological information with another service or with a health, police, private sector or other agency
- a primary school passing details about under-performing children to a social services department;
- two services exchanging information to promote one of the authority's services;
- two local authorities sharing information about their employees for fraud prevention purposes;
- a school providing information about pupils to a research organisation;

Who should use this code of practice?

Anyone who is involved in the sharing of personal data should use this code to help them to understand how to adopt good practice. While some parts of the code are necessarily focussed on sector-specific issues, the majority of the good practice recommendations will apply to all data sharing regardless of its context and scale.

How the code can help

Adopting the good practice recommendations in this code will help you to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing. The code will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits of this code include:

- ensuring that data sharing is fair, lawful and accountable and complies with Data Protection law;
- inspiring public trust by helping ensure that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- greater trust and a better relationship with the people whose information you want to share;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent or in the face of objection;

- minimised risk of breaches and consequent enforcement action by the ICO or other regulators; and
- reduced risk of questions, complaints and disputes about the way you share personal data.

Data sharing and the law

Before sharing any personal information you hold, you will need to consider all the legal implications of doing so. This is the case whether or not the information you wish to share is personal data because your ability to share information is subject to a number of legal constraints which go beyond the requirements of the Data Protection Act.

If you wish to share information with another person or body/agency, whether by way of a one-off disclosure or as part of a large-scale information sharing arrangement, you need to consider whether you have the legal power to do so and the purpose for sharing the information. This is likely to depend, in part, on the nature of the information in question – for example whether it is personal data or other confidential data. However, it also depends on who 'you' are, because your legal status also affects your ability to share information.

The public sector

Most public sector organisations, other than government departments headed by a Minister of the Crown, derive their powers entirely from statute – either from the Act of Parliament which set them up or from other legislation regulating their activities. Your starting point in deciding whether any information sharing initiative may proceed should be to identify the legislation that is relevant to the Council. Even if this does not mention information sharing explicitly, and usually it will not do so, it is likely to lead you to the answer to this question. With respect to west Lothian Council, relevant sources of legislation include:

Local Government (Scotland) Act 1994:
http://www.legislation.gov.uk/ukpga/1994/39/contents

Local Government Act 2000: http://www.legislation.gov.uk/ukpga/2000/22/contents
(especially sections relating to Access to information)

Civic Government (Scotland) Act 1982: http://www.legislation.gov.uk/ukpga/1982/45

Regulation of Investigatory Powers (Scotland) Act 2000:
http://www.legislation.gov.uk/asp/2000/11/contents

Freedom of Information (Scotland) Act 2002:
http://www.legislation.gov.uk/asp/2002/13/contents

Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Contacts within West Lothian Council

Data Protection Officer, Julie Whitelaw, West Lothian Civic Centre
Email: dpo@westlothian.gov.uk

Legal services Carol Johnston, Chief Solicitor, West Lothian Civic Centre
Email: Carol.Johnston@westlothian.gov.uk

The relevant legislation will probably define the Council's functions in terms of its purposes (the things that it *must* do), and the powers which the organisation may exercise in order to achieve those purposes (the things that it *may* do). So it is necessary to identify where the information sharing in question would fit (if at all) into the range of things that the Council is able to do. Broadly speaking, there are three ways in which it may do so:

- **Express obligations** – Occasionally, the Council will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances but, where such an obligation applies, it is clearly permissible to share the information. The *manner* in which the information is shared must still comply with other legal duties, including those in the Data Protection law if the information is personal data.

- **Express powers** – Sometimes, the Council will have an express power to share information. Again, an express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".

- **Implied powers** – Often, the legislation regulating the Council's activities is silent on the issue of information sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. To decide if you can rely on an implied power, you will need to identify the activity to which the proposed information sharing would be "reasonably incidental", and then check that the organisation has the power to engage in that activity. If in doubt, seek appropriate advice.

Whatever the source of the Council's authority to share information, you must obviously check that this covers the particular disclosure or information sharing arrangement in question: otherwise, you must not share the information unless, in the particular circumstances, there is an exemption in the Data Protection legislation which allows disclosure to take place. This might be the case where there are child protection or adult protection issues.

Within West Lothian there are clearly published information sharing protocols which underpin the legal obligations for information sharing within the organisation and with external agencies.

Link to Pan Lothian Partnership – General Protocol for Sharing Information document

Ultimately decisions relating to management of information and security lie with the relevant heads of service within the Council, with advice from legal services. At a service level the Information Liaison Officers (ILOs) for each service area will support and respond to any enquiries relating to information and security management. In the instance of a query about data sharing, your service ILO should be your first point of contact.

In cases specific to data sharing, ILOs and legal services will support senior management in relation to enquiries and clarifications.

The private sector

Before disclosing or sharing information with, or held by a private sector organisation, you must also be able to identify a power which permits the Council to do so. A private sector organisation's powers are likely to be set out in, or to derive from, its constitutional documents, such as a company's memorandum of association, rather than statute.

Private sector organisations will be required to adhere and subscribe to the overarching information sharing protocols (see previous section) and also to follow the guidelines and principles set out within this document.

Third party contractors who may be working with or have access to sensitive data will be required to adhere and subscribe to the Council contracts relating to confidentiality and also to follow the guidelines set out within this document.

Human rights

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature. Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal data. Article 8 is not an absolute right – public authorities are permitted to interfere with it if it is lawful and proportionate to do so.

It is advisable to seek legal advice if the disclosure or information sharing arrangement you are proposing engages Article 8 or any other Convention right. However, if you disclose or share personal data only in ways that comply with the Data Protection Act, the sharing or disclosure of that information is also likely to comply with the HRA.

Deciding to share personal data

When deciding whether to share personal data you need to identify the objective that it is meant to achieve. You should consider the potential benefits and risks, either to individuals or society, of sharing the information. You should also assess the likely results of not sharing the data. You should ask yourself:

- What is the sharing meant to achieve? You should have a clear objective, or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document this.
- Is your sharing of personal data in the public interest? This means that you should be able to justify it in terms of the benefit it brings to particular individuals, groups or society more widely.
- What information needs to be shared? You shouldn't share all the personal data you hold about someone if only certain data items are needed to achieve your objectives.
- For example, you might need to share somebody's current name and address but not other information you hold about them.
- Who does it need to be shared with? You should employ „need to know" principles, meaning that other organisations should only have access to your data if they need

it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onwards sharing of data with third parties.

- When should it be shared? Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- How can we check the sharing is achieving its objectives, and judge whether information sharing is still appropriate and that the safeguards still match the risks?
- What risk does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals‟ trust in the organisations that keep records about them?
- Could the objective be achieved without sharing the data or by anonymising it? The rules of data protection mean that you are only allowed to process personal data when it is necessary to do so, unless the subject agrees otherwise. In effect, this means that it is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

FAIRNESS, TRANSPARENCY AND CONSENT

Data Protection Law requires that personal data be processed fairly. This means that people should be aware that the Council is sharing their personal data, who with and what it is being used for and they should expressly consent to this. You need to think about this before you first share any personal data. This applies equally to routine information sharing or a single, one-off disclosure.

There are exceptions to fairness and transparency standards – these are explained in the ICO Guide to Data Protection which can be found on the ICO website at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

However, the general rule is that your sharing of personal data must be lawful, fair and transparent.

Privacy notices

The ICO has already produced comprehensive good practice guidance on the drafting and distribution of privacy notices (sometimes known as fair processing notices) More information on transparency and privacy notices is available on the ICOs web site:

https://ico.org.uk/for-organisations/

Much of the guidance on privacy notices is particularly relevant in data sharing contexts because of the need to ensure that people know which organisations are sharing their personal data and what it is being used for.

In a data sharing context, a privacy notice should **at least** tell the individual:

- who you are, including details of the Data Protection Officer;
- a summary of the personal data;
- the legal basis for sharing personal data;
- how long the data will be kept for;
- what is the purpose of sharing personal data; and
- who you are going to share it with.

You should provide a privacy notice when you first collect a person's personal data. If you have already collected their personal data, then you need to provide them with the information above as soon as you decide that you're going to share their data or as soon as possible afterwards.

In some cases a single privacy notice will be enough to inform the public of all the data sharing that you carry out. However, if you are engaged in more than one data sharing activity, it is good practice to provide information about each one separately. This will allow you to give much more tailored information, and to target it at the individuals affected by the particular sharing. There is a danger that individuals affected by data sharing will not be able to find the information they need if the Council only publishes one all-encompassing privacy notice.

If your information sharing involves a number of different organisations, it is good practice where possible for the organisation that has the initial contact with the individual to provide a privacy notice on behalf of all the participants. However, it is also good practice for all the organisations involved in the sharing to be prepared to explain their involvement in the data sharing should an individual ask about it.

Information sharing arrangements can change over time – for example where a law is introduced that requires an organisation to take part in a new data sharing operation. As a result, it is good practice to review your privacy notice regularly so that it continues to reflect accurately the data sharing you are involved in. Any significant changes to your privacy notice need to be publicised appropriately – depending primarily on the impact of the changes on individuals.

Telling individuals about data sharing

Data Protection Law leaves it open as to how, or whether, you have to provide a privacy notice. In some cases it is enough just to have a privacy notice available so people can access it if they want to. This approach is acceptable where the information sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object.

It is good practice to communicate a privacy notice actively. This is a legal obligation where a failure to do so would result in unfairness to the individual. By "communicate actively" we mean taking a positive action to provide a Privacy Notice, for example by sending a letter, reading out a script or distributing an email.

A good way to decide whether to communicate a notice actively is to try to anticipate whether the individual would expect it to be shared or would object if they knew about it.

The need to communicate a privacy notice actively is strongest where:

- You are sharing sensitive personal date; or
- The data sharing is likely to be unexpected or objectionable; or
- Sharing the data, or not sharing it, will have a significant effect on the individual; or
- The sharing is particularly widespread, involving organisations individuals might not expect such as partner agencies; or
- The sharing is being carried out for a range of different purposes

Who should tell the individual?

Data sharing typically involves personal data being disclosed between a number of organisations and services, all of whom have a responsibility to comply with Data Protection law, including its fairness provisions.

The most important thing is to ensure that the organisations involved in data sharing work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for, or will be used for. The primary responsibility for doing this falls to the organisation that collected the data initially. However, it is good practice for all the organisations or services areas involved to ensure that, throughout the data sharing process, individuals remain aware of who has their personal data and what it is being used for. This is particularly important where the data has been disclosed to an organisation the individual might not expect it to be shared with or where it is being used for a different purpose. It is good practice for recipients of personal data to check the privacy notice of the organisation that collected the data originally, to check whether it describes the recipient and its use of the data.

Consent

If there is no statutory requirement or authority to share personal data, you must ensure that you have explicit consent to share the personal data.

You must be sure that individuals know precisely what data sharing they are consenting to being shared and that they understand the implications for them. They must also have genuine control over whether or not the data sharing takes place. It is not appropriate to ask for consent to share if the data sharing is going to take place regardless of their wishes, for example where it is required by statute or is necessary for the provision of an essential service.

Consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a legislative requirement to do so;
- the individual would be likely to object should the data be shared without his or her consent; or

- the sharing is likely to have a significant impact on an individual or group of individuals.

You should remember that Data Protection law does not always require consent in order to legitimise the sharing of personal data. The legislation provides various alternatives to consent.

Further conditions within the Data Protection law are outlined on the ICO website at:
www.ico.gov.uk/for_organisations/data_protection/the_guide/conditions_for_processing.aspx

Sharing without the individual's knowledge

The general rule in Data Protection law is that individuals should, at least, be aware that personal data about them has been, or is going to be, shared – even if their consent for the sharing is not needed. However, in certain limited circumstances Data Protection law provides for personal data, even sensitive data, to be shared without the individual even knowing about it. Further information on these circumstances can be found on the ICO website at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

For example, you should not need to tell an individual that data about them has been shared with the police if this would allow them to destroy evidence, prejudicing a criminal investigation.

In some cases the sharing of data is required by law, for example under the Money Laundering Regulations 2007 – these allow financial institutions to share personal data with law enforcement agencies in certain circumstances. Such legal requirements can override an individual's consent or objection. However, it is still good practice, and may still be a legal obligation, to explain in general terms the circumstances in which personal data will be shared and the likely consequences for individuals.

It is also good practice to tell the individual as soon as you can after the risk of prejudice has passed that information about them has been shared. However, secrecy may be maintained where this would be likely to prejudice future policing operations, for example.

It is good practice to document any decisions you have taken regarding the sharing of personal data without the individual's knowledge, including the reasons for those decisions. This is important in case there is a challenge to your decision to share data, for example in the form of a complaint to the ICO or a claim for compensation in the courts.

> In West Lothian Council there exist a *number of consent forms and defined local* consent policy to ensure adherence to best practice when processing personal or sensitive personal data.

Link to Information Sharing Consent Form (example from Single Shared Assessment)
Link to Single Shared Assessment Joint System Consent document

Ad hoc or 'one-off' data sharing

Much data sharing takes place in a systematic, pre-planned and routine way. As such, it should be governed by established rules and procedures. However, sometimes a quite unexpected need to share someone's personal data may arise – for example in an emergency situation. In such cases the Council cannot be expected to have detailed procedures in place, and may just have to go ahead and make a decision about disclosure in the circumstances of the case, possibly in conditions of real urgency. Data Protection law provide various exemptions that allow ad hoc data sharing to take place lawfully. Further information on the exemptions can be found on the ICO website at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

Sometimes there may be a need to share very sensitive or confidential information, even without the individual's knowledge. Acting appropriately in situations like this depends primarily on the exercise of professional judgement. However, disclosures of personal data in situations like this are still subject to Data Protection law. The ICO will give due weight to compliance with authoritative professional guidance in determining whether there has been a breach of Data Protection law. Therefore it is very much in the interests of the Council and individual employees to be aware of any professional guidance or ethical rules that are likely to be relevant to the type of decisions about disclosing personal data that they may be asked to make.

SECURITY

Data Protection law requires organisations to have appropriate technical and organisational measures in place when sharing personal data. Organisations may be familiar with protecting information they hold themselves, but establishing appropriate security in respect of shared information may present new challenges.

Within West Lothian there is a corporate information register where all instances of information sharing should be logged. Please contact your Information Liaison Officer if you have any questions regarding the register.

It is good practice to take the following measures in respect of information that you share with other organisations, or that other organisations share with you.

- Review what personal data your organisation receives from other organisations, making sure you know its origin and whether any conditions are attached to its use.
- Review what personal data your organisation shares with other organisations, making sure you know who has access to it and what it will be used for.
- Assess whether you share any data that is particularly valuable, or is sensitive or confidential. Make sure you afford this data appropriate security.
- Identify who has access to information that other organisations have shared with you; "need to know" principles should be adopted. You should avoid giving all your staff access to shared information if only a few of them need it to carry out their job.
- Consider the effect a security breach could have on individuals.
- Consider the effect a security breach could have on your organisation in terms of

cost, reputational damage or lack of trust from your customers or clients. This can be particularly acute where an individual provides their data to an organisation, but a third party recipient organisation then loses the data.

It is important to build a culture of security awareness and good practice within any organisation, especially in respect of data received from another organisation or service area. Staff should be aware of security policies and procedures and be trained in their application. In particular steps must be taken to:

- design and organise security to fit the type of personal data disclosed or received and the harm that may result from a security breach;
- be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security. They should meet regularly to ensure appropriate security is maintained;
- have appropriate monitoring and auditing procedures in place; and
- be ready to respond to any failure to adhere to an information sharing protocol swiftly and effectively.

Within West Lothian all staff are required to adhere to the Information Governance Policy and the Information Security Guidance.

When personal data is shared, it is good practice for the organisation disclosing it to make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The organisation disclosing the information should ensure that the receiving organisation understands the nature and sensitivity of the information. It is good practice to take reasonable steps to ensure that those security measures are in place, for example by visiting premises periodically to check that security procedures are being adhered to. Please note, though, that the organisations the data is disclosed to will take on their own legal responsibilities in respect of the data, including its security.

Difficulties can arise when the organisations involved have different standards of security and security cultures or use different protective marking systems. It can also be difficult to establish common security standards where there are differences in organisations IT systems and procedures. Any such problems should be resolved before any personal data is shared. It is good practice for organisations sharing personal data to establish common security arrangements and to document these in their information sharing agreement.

There should be clear instructions about the security steps which need to be followed when sharing information by a variety of methods, for example phone, fax, email or face-to-face. It is also important that the recipient of the information understands the security implications and obligations that holding this information places on them to ensure that the information remains properly protected.

GOVERNANCE

Responsibility

The various organisations involved in a data sharing initiative will each have their own responsibilities, and liabilities, in respect of the data they disclose or have received. The issues the data sharing is intended to address may be very sensitive ones, and the decisions staff members may have to take can call for great experience and sound judgement. Therefore it is good practice for a senior, experienced person in each of the organisations involved in the sharing to take on overall responsibility for information governance, ensuring compliance with the law, and providing advice to staff faced with making decisions about information sharing.

Data sharing agreements

Data sharing agreements, or protocols, set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. It is good practice to have a data sharing protocol in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

A data sharing agreement must, at least, document the following issues:

- the purpose, or purposes of the training;
- the parties to which the protocol applies;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- the data to be shared;
- data quality – accuracy, relevance, usability etc;
- data security;
- retention timescales of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness / termination of the sharing agreement;
- sanctions for failure to comply with the agreement or breaches by individual staff;
- key legislation applying to the terms of information sharing; and
- any consent considerations or requirements.

Suggested contents of a data sharing protocol

Data sharing protocols can take a variety of forms, depending on the scale and complexity of the data sharing in question. You should remember that a protocol is essentially a set of common rules applying to all the organisations involved in a data sharing initiative. This means that the protocol should be drafted in clear, concise language that is easily understood.

Drafting and adhering to a protocol does not provide any form of legal indemnity from action under Data Protection Law or other law. However, a protocol should help you to justify your data sharing and to demonstrate that you have been mindful of, and have documented, the

relevant compliance issues. The ICO will take this into account should it receive a complaint about your data sharing.

In order to adopt good practice and to comply with Data Protection Law, the ICO would expect a protocol to address the following issues:

Purpose of the data sharing initiative

Your protocol should explain why the data sharing initiative is necessary, the specific aims you have and the benefits you hope to bring to individuals or to society more widely. This should be documented in precise terms so that all parties are absolutely clear as to the purposes for which data may be shared and shared data may be used.

The organisations that will be involved in the data sharing

Your protocol should identify clearly all the organisations that will be involved in the data sharing and should include contact details for their key members of staff. It should also contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.

Data items to be shared

You should explain the types of data that you are intending to share with the organisations stated above. This may need to be quite detailed, because in some cases it will be appropriate

You need to clearly explain the basis upon which you are sharing data. The Council may be under a legal duty to share certain types of personal data. Even if you are not under any legal requirement to share data, you should explain the legal power you have which allows you to disclose or receive personal data.

If consent is to be a basis for disclosure then your protocol could provide a model consent form. It should also address issues surrounding the withholding or withdrawal of consent.

Access and individuals' rights

The protocol should explain what to do when the Council or any other party to the protocol receives a Data Protection or FOISA request for access to shared data. In particular, it should ensure that one staff member or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily. Although decisions about access will often have to be taken on a case by case basis, your protocol should give a broad outline of the sorts of data you will normally release in response to either Data Protection or FOISA requests. It should also address the inclusion of certain types of information in your FOISA publication scheme. Further guidance on a data controller's / public authority's responsibilities under Data Protection Law and FOISA is available on the ICO website at:

www.ico.gov.uk/for_organisations/data_protection.aspx

www.ico.gov.uk/for_organisations/freedom_of_information.aspx

Information governance

Your protocol should also deal with the main practical problems that may arise when sharing

personal data. This should ensure that all organisations involved in the sharing:

- have detailed advice about which datasets may be shared, to prevent irrelevant or excessive information being disclosed;
- make sure that the data being shared is accurate, for example by requiring a periodic sampling exercise;
- are using compatible datasets and are recording data in the same way. The protocol could include examples showing how particular data items – for example dates of birth – should be recorded;
- have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the protocol;
- have procedures for dealing with Data Protection or FOISA access requests, or complaints or queries, from members of the public;
- have a timescale for assessing the ongoing effectiveness of the data sharing initiative and of the protocol that governs it; and
- have procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

It might be helpful for your protocol to have an appendix, including:

- a glossary of key terms;
- a summary of the key legislative provisions, for example relevant sections of Data Protection Law, any legislation which provides your legal basis for data sharing and links to any authoritative professional guidance;
- a model form for seeking individuals‟ consent for data sharing; • a diagram to show how to decide whether to share data;
- a data sharing request form; and
- a data sharing request record sheet.

Things to avoid

- When sharing personal data there are some practices that you should avoid. These practices could lead to regulatory action:
- Misleading individuals about whether you intend to share their information. For example, not telling individuals you intend to share their personal data because they may object.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is shared for.
- Sharing personal information when there is no need to do so – for example where statistical information can be used to plan service provision.

- Not taking reasonable steps to ensure that information is accurate and up to date before you share it. For example, failing to update address details before sharing information leading to individuals being pursued at the wrong address or missing out on important information.
- 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 details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a general office number.

Template 'information request' form

West Lothian Council

Information Request Form

Name of requester	
Name of organisation	
Date of the request	
Date information is required by	

In accordance with the **[*insert name of information sharing protocol*]** I am requesting the following items of personal data from you for the purposes of:

Item1	
Item 2	
Item 3	
Item 4	

Signed: ……

Date: ……

Download an electronic version of this form from the intranet

Template 'record disclosure' form

West Lothian Council

Record of Disclosure Form

Name of requester	
Name of organisation	
Date request received	
Reference given for request	
Period of retention for shared data	
Arrangements for deletion or return of data:	
Information asked for:	
Reason(s) for disclosure or non-disclosure:	
Decision taken by	
Date of disclosure	

Signed: ……

Date: ……

Download an electronic version of this form from the intranet

Data Protection Impact Assessments (DPIAs)

Before entering into any data sharing arrangement, it is good practice to carry out a data protection impact assessment. This will help you to assess the benefits that the data sharing might bring to particular individuals or society more widely. It will also help you 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. As well as harm to individuals, you may wish to consider potential harm to the Council's reputation which may arise if data is shared inappropriately, or not shared when it should be. Data protection impact assessments are mandatory for Government Departments when introducing certain new processes involving personal data.

Further information on privacy impact assessments can be found on the ICO website: www.ico.gov.uk

APPENDICES

Data Standards (Annex 1)

Data Protection principles (see Annex 3) provide a framework which organisations involved in data sharing should use to develop their own information governance policies. It is important to have procedures in place to maintain the quality of the personal data you hold, 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 take account of the following considerations:

Make sure that the format of the data you share is compatible with the systems used by both organisations.

Different organisations may use very different IT systems, with different hardware and software and different procedures for its use. This means that it can be very difficult to „join" systems together in order to share personal data properly. These technical issues need to be given due weight when deciding whether, or how, to share personal data.

Organisations may also record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mismatched or becoming corrupted. There is a risk that this will cause detriment to individuals if holding an incomplete record means that you do not provide services correctly. Before sharing information you must make sure that the organisations involved have a common way of recording key information, for example by deciding on a standard format for recording people's names. A relatively common problem here is the recording of names which contain non-Latin characters. Each organisation might have its own way of recording these, depending on the capabilities of its system. If you cannot establish a common standard for recording information, you must develop a reliable means of converting the information.

If the characters in a dataset are encoded using a different system, they might not transfer correctly. You should ensure that the data is compatible with both systems, especially in cases which are more likely to use non-standard characters.

Given the problems of interoperability that can arise, it is good practice for organisations that are likely to be involved in data sharing to require common data standards as part of their procurement exercises. IT suppliers should be made aware of these requirements.

Example data standards policies can be found below:

- Government data standards catalogue.
- Local government data standards.
- NHS data standards and products.

Check that the information you are sharing is accurate before you share it.

Before you share data you should take steps to check its accuracy. After the information has been shared it can be difficult to have it amended, so you should do as much as you can

prior to disclosure. The steps you take should depend on the nature of the data involved. If you are sharing sensitive data and any inaccuracy would potentially harm the data subject, you will need to take extra care to ensure that the information is correct.

It is good practice to check from time to time whether the information being shared is of good quality. For example, a sample of records could be looked at to make sure the information contained in them is being kept up to date. The larger the scale of the data sharing, the more rigorous the sampling exercise should be. It is a good idea to show the records to the people they are about so that the quality of information on them can be checked. Although this may only reveal deficiencies in a particular record, it could indicate wider systemic failure that can then be addressed.

Establish ways for making sure inaccurate data is corrected by all the organisations holding it.

You should ensure that procedures are in place for amending data after it has been shared. This might be because the data subject notifies you of an inaccuracy, or because they have asked you to update their details. The action you need to take will depend on the circumstances of each case. If the data is intended for ongoing use then it could be necessary for all the organisations holding it to amend it.

If several organisations are sharing information in a partnership, they should establish who is responsible for maintaining the accuracy of the data and responding to any complaints or requests for amendment.

Agree common retention periods and deletion arrangements for the data you send and receive.

The various organisations sharing personal data should have an agreement about what should happen once the need to share the data has passed. Where the information is held electronically the information should be deleted, and a formal note of the deletion should be sent. Where the particular issue that the data sharing was intended to deal with has been resolved, all the organisations involved should delete their copies of the information unless there is a requirement to retain it for another purpose, for example archiving. Paper records can cause particular problems. It can be easy to overlook the presence of old paper records in archives or filing systems – and they may well contain personal data subject to Data Protection law. Once the need to retain them has passed, paper records should be securely destroyed or returned to the organisation they came from.

The various organisations involved in a data sharing initiative may need to set their own retention periods for information. However, if shared data is no longer needed for the purpose for which it was shared, then all the organisations it was shared with should delete it. However, the organisation, or organisations, that collected the data in the first place may be able, or be required, to retain the original data for another legitimate purpose.

Some information will be subject to statutory retention periods and these must be adhered to. You must make sure that any organisation that has a copy of the information also deletes it in accordance with statute.

If you can remove all identifying information from a dataset so that it no longer constitutes personal data, then it can be retained indefinitely.

Train staff so that they can share information appropriately and safely.

It is good practice to provide training on data sharing to staff that are likely to make decisions about data sharing or have access to shared data. The nature of the training will depend on their role in respect of the sharing of personal data. It can be incorporated into any training you already give on data protection, security, or legal obligations of staff.

Different types of staff involved in data sharing will have different training needs, depending on their role. Those who:

- plan and make decisions about systematic sharing;
- administer systematic systems; or
- who make decisions in one off situations

will each have different requirements based on their responsibilities.

The focus of the training should be enabling staff to make informed decisions about whether or how to share data, and how to treat the data they are responsible for.
People who have overall responsibility for data sharing need to understand:

- the relevant law surrounding data sharing, including the Data Protection Act 2018;
- any relevant professional guidance or ethical rules;
- data sharing protocols and the need to review them;
- how different information systems work together;
- security and authorising access to systems holding shared data;
- data quality checks; and
- retention periods for shared data.

They also need the seniority and influence to make authoritative decisions about data sharing.

Reviewing your data sharing arrangements

Information sharing must be necessary, proportionate and have a positive outcome for individuals or for society more widely. Therefore, once you have an information sharing arrangement in place it is very important to review it on a regular basis. This is because changes can occur and they need to be reflected in your arrangements to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

You should ask yourself the following key questions regularly:

- Is the data still needed? You may find that the aim of the information sharing has been achieved and that no further sharing is necessary. On the other hand, you may find that the information sharing is making no impact upon your aim and therefore the sharing is no longer justified.

- Do your privacy notice and any data sharing protocols you have in place still explain accurately the data sharing you are carrying out? Please see the fairness and transparency section of this code and section 14 on data sharing protocols for further information. It is good practice to check that your information governance procedures are still adequate and are working in practice. All the organisations involved in the sharing should check:

    - whether it is necessary to share personal data at all, or whether anonymised information could be used instead;
    - that only the minimum amount of data is being shared and that the minimum number of organisations, and their staff members, have access to it;
    - that the data shared is still of appropriate quality;
    - that retention periods are still being applied correctly by all the organisations involved in the sharing;
    - that all the organisations involved in the sharing have attained and are maintaining an appropriate level of security; and
    - that staff are properly trained and are aware of their responsibilities in respect of any shared data they have access to.

- You should check that you are still providing people with access to all the information they're entitled to, and that you're making it easy for them to access their shared personal data.
- You should check that you are responding to people's queries and complaints properly and are analysing the information to make improvements to your data sharing arrangements.

If significant changes are going to be made to your information sharing arrangements then those changes need to be appropriately publicised. This can be done by updating websites, sending emails directly to people or, if appropriate, advertisements in local newspapers.

Individuals' Rights (Annex 2)

Data Protection law gives individuals certain rights over their personal data. These include:

- the right to access personal data held about them;
- the right to know how their data is being used; and
- the right to object to the way their data is being used.

Access to information

The Council is required by law to give people access to data about them in a permanent form. (WLC policy not to charge) You can find more advice on responding to requests through the ICO Guide to data protection.

- You should provide clear information for individuals about how they can access their data and make this access as straightforward as possible.
- You must be able to locate and access personal data you are responsible for promptly in order to respond to requests.
- When you receive a request from an individual for their personal data you must respond to the request promptly and in any event within 40 days.

When several organisations are sharing personal data it may be difficult for an individual to decide who they should make a request for information to. You should provide clear information about the way in which individuals can make requests. It is good practice to provide a single point for individuals to direct their access requests to, allowing them to access the data that has been shared between several organisations without making multiple requests.

It is good practice to provide ways for people to access and check their own data without needing to make a formal request. You could do this by setting up facilities to allow records to be viewed online, if this can be done securely, or by showing people their data when you are in contact with them. Providing these options could save you time responding to formal requests and help to ensure the data you hold is accurate and up to date.

Where personal data is shared between several bodies it can be difficult to determine who is responsible for the data and what exactly is held. It is very important that organisations sharing data manage their records well to ensure they can locate and provide all the data held about a person when they receive an access request.

When responding to a request for personal data an organisation is also required by law to provide a description of the purposes for which the data is held and details of the recipients or types of recipients - who the data is disclosed to. Providing this detail is particularly important where data is being shared so that individuals are reminded about the ways their information is being used and disclosed. It also makes it easier for them to take action where they think an organisation has disclosed their data to another organisation inappropriately.

You are also required to provide any information you have about the source of the data you hold. In some cases this information may have been provided by another individual. This might be the case, for example, where a child's social work file contains information provided by a concerned neighbour. In cases like this, there is likely to be a clear basis for information about the source to be withheld. The ICO subject access information guidance contains more detail on this subject.

In certain cases you may be responsible for replying to a request for personal data which was shared with you but you may not be in a position to make the judgement about whether a particular exemption should be applied. For example you may be concerned about the impact of releasing a report containing information prepared by a doctor about an individual's health. The decision about whether disclosing this information could cause serious harm to the individual would need to be made by a medical professional. In this instance you would need to seek advice from the doctor who prepared the report or another medical professional if this is not possible.

Individuals' objections

Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or substantial, unwarranted distress. The objection can be to a particular use of information or to the fact an organisation is holding their personal data at all. Organisations are required by law to respond to individuals who object in writing to the way their personal data is being used. However they do not need to comply with the request unless the damage or distress is substantial and unwarranted.

You could avoid objections by providing individuals with clear information about the basis on which you are sharing their personal data and the ways it will be used.

- When you receive a request from an individual to stop using their information you must respond to them within 21 days to confirm what action you intend to take.
- If you consider their objection unwarranted you should let them know and provide clear reasoning for your decision.
- If you are taking action to comply with the individual's request you should explain the steps you are going to take and provide a timescale.

In Data Protection law the right to object is linked to the likelihood of substantial and unwarranted damage or distress being caused. This means that the individual has no unqualified right to stop their personal data being shared.

Queries and complaints

Individuals may have queries or complaints about how their personal data is being shared, particularly where they think the data is wrong or that the sharing is having an adverse effect on them. It is good practice to have procedures in place to deal with any queries or comments you receive in a quick and helpful way, for example by having a single point of contact for members of the public. It is good practice to analyse the comments you receive in order to develop a clearer understanding of public attitudes to the information sharing you carry out. Answering individuals 'queries can also allow you to provide further information about your data sharing, in addition to what's contained in your privacy notice.

If you inform people about your data sharing and then receive a significant number of objections, negative comments or other expressions of concern, you should review the data sharing in question. In particular, you should analyse the concerns raised and decide whether the sharing can go ahead in the face of public opposition, for example because you are under a legal obligation to share the data. Alternatively, you may need to reduce the amount of data you share or share it with fewer organisations. In large-scale data sharing operations, it is good practice to set up focus groups to explore individuals‟ concerns and to develop more publicly acceptable ways of dealing with the issues that the data sharing was intended to address.

ICO Powers and Penalties (Annex 3)

The ICO aims to make compliance with Data Protection law easier for the majority of organisations who want to handle personal data well. In cases where organisations do not comply the ICO has powers to take action to change behaviour. These powers include the ability to serve an enforcement notice, to conduct audits and to serve a monetary penalty notice. The tools are not mutually exclusive. They will be used in combination where justified by the circumstances.

The main options are:

- Information Notice: an Information Notice requires organisations to provide the ICO with specified information within a certain time period.
- Undertaking: an undertaking commits an organisation to a particular course of action in order to improve its compliance with Data Protection law.
- Enforcement Notice: an enforcement notice compels an organisation to take the action specified in the notice to bring about compliance with Data Protection law. For example, a notice may be served to compel an organisation to start complying with subject access requests in the timescale required or a notice may require an organisation to take steps to prevent security breaches. Failure to comply with an enforcement notice is a criminal offence.
- Monetary Penalty Notice: a monetary penalty notice requires an organisation to pay a monetary penalty of an amount determined by the ICO, up to a maximum of
- The ICO has the power to impose a civil monetary penalty (CMP) on a data controller of up to £17million (20m Euro) or 4% of global turnover. This power can be used if:
    - an organisation has seriously contravened the data protection principles, and
    - the contravention was of a kind likely to cause substantial damage or substantial distress.

In addition the contravention must either have been deliberate or the organisation must have known, or ought to have known, that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

More guidance on the circumstances in which the Information Commissioner will use this power including what will be considered a “serious breach” can be found in the ICO’s website (see www.ico.gov.uk).

Audit: the ICO can conduct consensual or compulsory audits (following the serving of an Assessment Notice). A compulsory audit would be used by the ICO to determine whether an organisation has complied or is complying with the data protection principles where risks are identified and an organisation is unwilling to consent to an audit.

A consensual audit can assess an organisation’s processing of personal information for the following of good practice. This includes a consideration of the legal requirements of the DPA and other relevant ICO codes and guidance. This will include the requirements of this code of practice.

The power to undertake compulsory audits currently only extends to government departments, other categories of persons and public authorities designated by order of the secretary of state.

The Assessment notices code of practice sets out the factors which will be considered when the ICO decides whether to pursue a compulsory audit and specifies how that audit process will be conducted.

The ICO takes a selective, proportionate and risk based approach to pursuing regulatory action. Action is driven by concerns about actual or potential detriment caused by failure to comply with the DPA. The factors the ICO will take into account in determining whether regulatory action is appropriate are listed in the Data Protection Regulatory Action Policy.

Data Protection Act 2018 Fee (Annex 4)

The Data Protection Act 2018 requires that organisations that determine the purpose for which personal data is processed (controllers) must pay a data protection fee unless they are exempt. The new data protection fee replaces the requirement to 'notify' (or register) with the ICO.

Under data sharing arrangements the data controller and/or data processor responsibilities must be made clear. Where several organisations are sharing personal data it is important that each organisation is clear about their personal data responsibilities. With a few exemptions, all data controllers must pay a data protection fee to the ICO.

More information on data protection fees is available from the ICO web site.
https://ico.org.uk/for-organisations/data-protection-fee/

The ICO will publish details of all controllers who pay the data protection fee on the data protection register, available on the ICO website.

Freedom of Information (Annex 5)

The Freedom of Information (Scotland) Act 2002 (FOISA) gives everyone the right to ask for information held by a public authority and, unless exempt, to be told whether the information is held and to be provided with the information. In some cases, public authorities can refuse to confirm or deny whether they hold requested information. Advice on which organisations are public authorities under the Act can be found here:

http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.asp

The new INSPIRE Regulations contain provisions that deal specifically with the sharing of spatial data sets and spatial data services between public authorities For more information about this see: http://www.legislation.gov.uk/uksi/2009/3157/regulation/12/made

The FOISA requires every public authority to adopt and maintain a publication scheme, which is a commitment to publish information on a proactive and routine basis. This supports the culture of transparency introduced by freedom of information legislation and allows the public to easily identify and access a wide range of information without having to make a request.

Most, if not all, public sector bodies involved in data sharing are subject to freedom of information law. This means they are required to publish information in accordance with their publication scheme. The ICO introduced a model publication scheme that should be adopted by all public authorities subject to FOISA. The scheme became available for adoption on 1 January 2009. Further information on the scheme can be found here:

http://www.itspublicknowledge.info/ScottishPublicAuthorities/PublicationSchemes/PublicationSchemesHome.aspx

Public authorities are required to publish information covered by the model scheme's nine classes, and in accordance with class 5 they are required to publish their policies and procedures. In most cases this will include the policies and procedures relating to data sharing, including the details of the organisations with which data is shared and any relevant code of practice. Further information on the types of information public authorities are expected to make available through their schemes is available here:

http://www.itspublicknowledge.info/nmsruntime/saveasdialog.aspx?lID=11057&sID=8883

There is a strong public interest in members of the public being able to find out easily why data is being shared, which organisations are involved and what standards and safeguards are in place. Making your policies and procedures available to the public proactively should help to reassure individuals and to establish an increased level of trust and confidence in your organisation's information sharing practices. You should consider including details of data sharing with other public authorities within the policies and procedures that you publish in accordance with your publication scheme.

There will often be cases where data is shared with other public authorities. This will usually mean that the data is held for the purposes of the FOISA by all the data sharing partners and an FOI request could be made to any of the public authorities that hold the information. However, within the FOISA there is an exemption for the personal information of third parties that falls within the scope of a request. In many cases this exemption will apply as disclosure is likely to be unfair and so be in breach of the first data protection principle.

Often people will make requests for information that cover both personal and non-personal information. For example, a person may request data about them that is being shared

between various agencies and information about those agencies‟ policies for sharing information. Data protection and freedom of information may be dealt with by separate parts of your organisation, and a hybrid request may have to be dealt with under both pieces of legislation. However, it is good practice to be as helpful as possible when dealing with requests of this sort, especially as members of the public may not understand the difference between a data protection and an FOI request.

There may be circumstances where a private or third sector organisation shares data with a public authority. It is therefore important that, in such cases, individuals are made aware that information they provide will also be held by an organisation that is subject to the FOISA and so may fall within the scope of a request for information made to the public authority. However, as mentioned previously, there is an exemption within the FOISA for the personal data of third parties to which a request for information relates. In many cases this exemption will apply as disclosure is likely to be unfair and so be in breach of the principle that personal data must be processed fairly and lawfully.

The Data Protection Principles (Annex 6)

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. Personal data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')." "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.