The Moray Council

Data Sharing Code of Practice

Based on the Code of Practice issued by the Information Commissioners Office (ICO) on data sharing.

2013

Document Control Sheet

Name of Document:	**Data Sharing Code of Practice**
Author:	Eleanor Rowe, Records Manager
Consultees	Denise Whitworth, Head of HR & ICT Morag Smith, Senior Solicitor , Legal Services Mike Alexander, ICT Project Leader - Security Officer
Description of Content:	The purpose of this document is to give a local, Moray Council specific version and interpretation of the Code of Practice issued by the Information Commissioners Office (ICO) on data sharing.
Distribution:	Council wide upon approval
Status:	Version 0.1 DRAFT

Contents

1.0 Introduction

The purpose of this document is to give a local, Moray Council specific version and interpretation of the Code of Practice issued by the Information Commissioners Office (ICO) on data sharing.
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

This data sharing code of practice should be referenced in all and any instances of information and data sharing with Moray Council and external partners including NHS, police and other local authorities.

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 organisations that share personal data.

2.0 How the code of practice can help

Adopting the good practice recommendations in this code will help the Council 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 for organisations include:

- minimised risk of breaking the law and consequent enforcement action by the ICO or other regulators;
- better public trust by ensuring that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- increased data sharing when this is necessary and beneficial;
- 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; and
- reduced risk of questions, complaints and disputes about the way you share personal data.

3.0 The 8 Data Protection Act Principles

1. "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".

2. “Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”.

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 processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

6. “Personal data shall be processed in accordance with the rights of data subjects under this Act”.

7. “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”.

8. “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.

4.0 Data sharing & the Moray Council

By ‘data sharing’ we mean the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

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

Some data sharing doesn’t involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither the Data Protection Act (DPA), 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
- exceptional, ad hoc, 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.

4.1 Systematic data sharing

Much data sharing takes place in a pre-planned and routine way. As such, it should be governed by established rules and procedures. This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

Specific data sharing guidance and protocols are available from Legal Services.

4.2 Exceptional, Ad hoc or 'one-off' data sharing

The council may decide, or be asked, to share data in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

4.3 Sharing within the Council

Most staff will understand that data sharing refers to data between organisations. However, the data protection principles also apply to the sharing of information within an organisation – for example between the different departments of a local authority. Whilst not all the advice in this code applies to sharing within organisations, much of it will, especially as the different parts of the same organisations can have very different approaches to data protection, depending on their culture and functions.

5.0 Data sharing and the law

Before sharing any personal data you hold, you will need to consider all the legal implications of doing so. Your ability to share information is subject to a number of legal constraints which go beyond the requirements of the Data Protection Act (DPA). There may well be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect your ability to share personal data. A duty of confidence may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical or banking information, for example.

If you wish to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, you need to consider whether you have the legal power or ability to do so. This is likely to depend, in part, on the nature of the information in question – for example whether it is sensitive personal data. However, it also depends on who 'you' are, because your legal status also affects your ability to share information – in particular it depends on whether you are a public sector body or a private/third sector one. The starting point in deciding whether any data sharing initiative may proceed should be to identify the legislation that is relevant to your organisation.

Within Moray Council there are published data sharing protocols which underpin the legal obligations for information sharing within the organisation and with external agencies.

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 .Separate data processing agreements may also be required if information is being processed on our behalf.

See - Pan Grampian Data Sharing Partnership –Protocol for Sharing Information
http://www.moray.gov.uk/downloads/file64267.pdf

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 first contact point for data sharing will be the Corporate Policy Unit who manage data protection and FOI(S)ASA enquiries.

Contacts:-
Peter Jones, Corporate Policy Unit
Morag Smith, Legal Services
Eleanor Rowe, Records Manager
Mike Alexander, ICT Security Officer

6.0 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.

Legal Services will give advice on this.

7.0 Deciding to share personal data

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) 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 data. 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.
- 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 requires access to the shared personal data? 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 onward 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? You will need to judge whether it is still appropriate and confirm 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? 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.
- The council also needs to ensure that the sharing is covered in our register entry. Will any of the data be transferred outside of the European Economic Area (EEA)? If any data is to be transferred outside of the so, you need to consider the requirements of the eighth principle of the Data Protection Act (DPA). For more detailed guidance on this area see: www.ico.gov.uk Conditions for processing

7.1 Sharing Non Sensitive Personal Data

Conditions that provide a basis for processing non-sensitive personal data include:

- The processing is necessary:
  - in relation to a contract which the individual has entered into;
- or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.
- The 'legitimate interests' condition provides grounds to process personal data in a situation where an organisation needs to do so for the purpose of its own legitimate interests or the legitimate interests of the third party that the information is disclosed to.

This condition cannot be satisfied if the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the individual whose data is being processed. This condition cannot legitimise the processing of sensitive personal data.

7.2 Sharing Sensitive Personal Data

7.2.1 Definition of Sensitive personal data

1. personal data consisting of information as to a person's
2. racial or ethnic origin of the data subject
3. political opinions
4. religious beliefs or other beliefs of a similar nature
5. trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
6. physical or mental health or condition
7. sexual life
8. the commission or alleged commission of any offences

The first data protection principle says that organisations have to satisfy one or more 'conditions' in order to legitimise their processing of personal data, unless an exemption applies. Organisations processing sensitive personal data, for example information about a person's health, will need to satisfy a further, more exacting condition. It is important to be clear that meeting a condition for processing will not in itself ensure that the sharing of personal data is fair or lawful.

8.0 Sharing without the individual's knowledge

The general rule in the DPA 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 the DPA provides for personal data, even sensitive data, to be shared without the individual even knowing about it.

You can share without an individual's knowledge in cases where, for example, personal data is processed for:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of tax or duty.

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 override an individual's consent or objection. Secrecy may be maintained where this would be likely to prejudice future policing operations.

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.

Access to third party information guidance
http://intranet.moray.gov.uk/Information_management/DPA%20Guidance%20on%203rd%20party%20access%20for%20staff%20v1%200%20Dec%202012.pdf

Access to third party information application form
http://intranet.moray.gov.uk/Information_management/Documents/Access%20Form%20to%20Third%20Party%20Information.docx

Sometimes there may be a need to share very sensitive 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 the DPA. The ICO will give due weight to compliance with authoritative professional guidance in determining whether there has been a breach of the DPA. Therefore it is very much in the interests of organisations 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. It may not always be possible to document the sharing in an emergency or time dependent situation, however it is good practice to make a record as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place.

9.0 Consent

Consent (explicit consent for sensitive personal data) is one of the conditions the DPA provides to legitimise processing. The Data Protection Directive on which the UK's DPA is based defines 'the data subject's consent' as:

> 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

There must therefore be some form of active communication where the individual knowingly indicates consent. Whilst consent will provide a basis on which organisations can share personal data, the ICO recognises that it is not always achievable or even desirable. If you are going to rely on consent as your condition you must be sure that individuals know precisely what data sharing they are consenting to and understand its implications for them. They must also have genuine control over whether or not the data sharing takes place. It is bad practice to offer individuals a 'choice' 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 or explicit consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing 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.

The conditions for processing sensitive personal data are more difficult to satisfy. For example if you want to process medical data you have to satisfy a condition from the list above and also a

more stringent sensitive data condition – one of which specifically legitimises processing of health data for medical purposes, including the provision of treatment and medical research. For more details of all the conditions for processing and the circumstances in which they apply see the Guide to data protection: www.ico.gov.uk
Consent Form
http://www.moray.gov.uk/downloads/file41453.doc

Access to third party information guidance
http://intranet.moray.gov.uk/Information_management/DPA%20Guidance%20on%203rd%20party%20access%20for%20staff%20v1%200%20Dec%202012.pdf

Access to third party information application form
http://intranet.moray.gov.uk/Information_management/Documents/Access%20Form%20to%20Third%20Party%20Information.docx

10.0 Fair Processing of personal data

The Data Protection Act (DPA) requires that personal data be processed fairly. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for. In a broader sense, fairness also requires that where personal data is shared, this happens in a way that is reasonable and that people would be likely to expect and would not reasonably object to if given the chance.

10.1 Privacy notices [fair processing notice]

http://intranet.moray.gov.uk/Information_management/Documents/The%20Moray%20Council%20Privacy%20Notice%20July%202013.pdf

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.

The DPA 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 data sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object. In other cases 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 their personal data 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 data
- the data sharing is likely to be unexpected or objectionable

- sharing the data, or not sharing it, will have a significant effect on the individual
- the sharing is particularly widespread, involving organisations individuals might not expect
- the sharing is being carried out for a range of different purposes.

11.0 Who should tell the individual?

Data sharing typically involves personal data being disclosed between a number of organisations, all of whom have a responsibility to comply with the DPA, 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.

12.0 Security

The Data Protection Act (DPA) 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.

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 sensitive. Make sure you afford this data a suitably high level of 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.
- You should aim to build a culture within your organisation where employees know and understand good practice, in respect of 'its own' data and that received from another organisation. Staff should be aware of security policies and procedures and be trained in their application. In particular you will need to design and organise your security to fit the type of personal data you disclose or receive and the harm that may result from a security breach
- The Moray Council's Information Assurance group is responsible for ensuring information security. They 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 a data sharing agreement swiftly and effectively.

ICT Security Policy
http://intranet.moray.gov.uk/documents/central_services/corporate_information_security_policy.pdf

Information Assurance Group
http://intranet.moray.gov.uk/Information_management/Documents/Information%20Assurance%20Group%20Remit.pdf

12.1 Physical security

Buildings are protected by access keys and secure access points. Staff wear id badges and visitors are required to sign in to buildings or are escorted by staff. Paper based information is stored and transferred securely. The council operates a clear desk policy and removable media and laptops should be locked away when not in use. The council have a confidential paper waste disposal contract.

12.2 Technical security

ICT will be responsible for the following data sharing considerations:-

Is your technical security appropriate to the type of system you have, the type of information you hold and what you do with it?

If you have staff that work from home, do you have security measures in place to ensure that this does not compromise security? See ICT Security Policy
http://intranet.moray.gov.uk/documents/central_services/corporate_information_security_policy.pdf

How is encryption of personal data implemented and managed?

Have you identified the most common security risks associated with using a web-product – e.g. a website, web application or mobile application?

How do you control access to your systems?

Do you set privileges to information based on people's need to know?
What measures are in place for the security of information in transit?

Access Control Policy EDRMS
http://intranet.moray.gov.uk/Information_management/Access%20Control%20Policy%20v1%200.pdf

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, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement. 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.

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.

13.0 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 data sharing.

14.0 Data Sharing Agreements or Protocols

Data sharing agreements – sometimes known as 'data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement 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 should, at least, document the following issues:

- the purpose, or purposes, of the sharing
- 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 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
- names, dates and signatures of approvers
- key legislation relevant to data sharing

14.1 Key elements of a data sharing agreement.

A data sharing agreement is a set of common rules binding on all the organisations involved in a data sharing initiative. This means that the agreement should be drafted in clear, concise language that is easily understood.

Drafting and adhering to an agreement does not in itself provide any form of legal indemnity from action under the Data Protection Act (DPA) or other law. However, an agreement 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 the DPA, the ICO would expect a data sharing agreement to address the following issues:

Purpose of the data sharing initiative:

Your agreement 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 agreement 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:

Your agreement 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 to share certain details held in a file about someone, but not other, more sensitive, material. In some cases it may be appropriate to attach ‘permissions’ to certain data items, so that only certain members of staff, for example ones that have received appropriate training, are allowed to access them

Basis for sharing:

You need to explain your basis for sharing data clearly. If you are a public sector body, you 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 share. If you are a private or third sector organisation then you may not need a specific legal power to disclose personal data, but your agreement should still explain how the disclosures will be consistent with the DPA.

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

Access and individuals' rights:

The agreement should explain what to do when an organisation receives a DPA or FOI(S)A 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 agreement should give a broad outline of the sorts of data you will normally release in response to either DPA or FOI(S)A requests. It should also address the inclusion of certain types of information in your FOI(S)A publication scheme.

Information governance:

Your agreement 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 agreement 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 for the transmission of the data and procedures for dealing with any breach of the agreement;
- have procedures for dealing with DPA or FOI(S)AA 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 agreement that governs it; •
- 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 agreement to have an appendix, including:

- a glossary of key terms;
- a summary of the key legislative provisions, for example relevant sections of the DPA, 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.

You may also want to consider including:

- a data sharing request form;

- a data sharing decision form.

Template 'data sharing request' form

Name of organisation:
Name and position of person
requesting data:
Data requested:
Reference to data sharing agreement:
Purpose:
Date required by:
Any specific arrangements re: retention/deletion of data:
Date of request:
Signed:
Dated:

Template 'data sharing decision' form

Name of organisation:
Name and position of person requesting data:
Date request received:
Data requested:
Purpose:
Decision:
Data supplied:
Reason(s) for disclosure or non-disclosure:
Any specific arrangements re: retention/deletion of data:
Decision taken by (name and position):
Date of disclosure:
Signed:
Dated:

Access to third party information guidance
http://intranet.moray.gov.uk/Information_management/DPA%20Guidance%20on%203rd%20party%20access%20for%20staff%20v1%200%20Dec%202012.pdf

Access to third party information application form
http://intranet.moray.gov.uk/Information_management/Documents/Access%20Form%20to%20Third%20Party%20Information.docx

15.0 Privacy impact assessments (PIAs)

Before entering into any data sharing arrangement, it is good practice to carry out a privacy 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 your organisation's reputation which may arise if data is shared inappropriately, or not shared when it should be. Further information on privacy impact assessments can be found on our website at: www.ico.gov.uk.

16.0 Data standards

The Data Protection Act (DPA) principles 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 consider the following issues:

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

For local government: http://standards.esd.org.uk

17.0 Accuracy & Data Quality

Check that the information you are sharing is accurate and up to date before you share it. 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. The council must establish ways for making sure inaccurate data is corrected by all the organisations holding it.

You should also 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.

18.0 Retention and Disposal

Partners should 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 use 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 the DPA. 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, perhaps because they work to different statutory retention periods. 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 a statutory retention period and this 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.

Moray Council retention schedule

http://intranet.moray.gov.uk/Information_management/Documents/Retention%20Schedule%20Scope%20and%20Explanation%20Oct%202013.pdf

http://intranet.moray.gov.uk/Information_management/Documents/Retention%20Schedules%20version%2015%2000%202013.pdf

19.0 Training

Train your staff so that they know who has the authority to share personal data, and in what circumstances this can take place. It is essential to provide training on data sharing to staff that are likely to make significant 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 systems or 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 DPA;
- any relevant professional guidance or ethical rules;
- data sharing agreements and the need to review them;
- how different information systems work together;
- security and authorising access to systems holding shared data;
- how to conduct data quality checks; and
- retention periods for shared data.

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

20.0 Reviewing your data sharing arrangements

Once you have a data sharing arrangement in place you should 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 data sharing has been achieved and that no further sharing is necessary. On the other hand, you may find that the data sharing is making no impact upon your aim and therefore the sharing is no longer justified.
- Do your privacy notice and any data sharing agreements you have in place still explain the data sharing you are carrying out accurately?
- Are your information governance procedures still adequate and 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.
- Have you checked 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?
- Have you checked that you are responding to people's queries and complaints properly and are analysing them to make improvements to your data sharing arrangements? If significant changes are going to be made to your data sharing arrangements, then those changes need to be publicised appropriately. This can be done by updating websites, sending emails directly to people or, if appropriate, placing advertisements in local newspapers.

21.0 Individuals' rights

The Data Protection Act (DPA) 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.

22.0 Access to information

Information about access rights is given on the council website under Information Management/Access to Information
http://www.moray.gov.uk/downloads/file41455.pdf

Subject Access Request Form
http://www.moray.gov.uk/downloads/file41452.pdf

Consent Form
http://www.moray.gov.uk/downloads/file41453.doc

23.0 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 you think 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 being shared for.
- Sharing personal data when there is no need to do so – for example where anonymised 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.

24.0 Notification

The Data Protection Act (DPA) requires that organisations provide the ICO with a description of the individuals or organisations to whom they intend or may wish to disclose personal data. The legal requirement is to provide a description of the recipient or the recipients of the data – this means types of organisation, not the names of specific organisations. The notification requirement does not include people to whom you may be required by law to disclose personal data in a particular case, for example where the police require a disclosure of personal data under a warrant.

When you intend to share personal data with another organisation or group of organisations you must check whether you need to update your notification to describe this. When any part of the notification entry becomes inaccurate or incomplete, for example because you are now disclosing information to a new type of organisation, you must inform the ICO as soon as practical and in any event within 28 days. It is a criminal offence not to do this.

Where several organisations are sharing personal data it is important that each organisation is clear about the personal data they are responsible for and include that information on their notification entry.

25.0 Freedom of Information (Scotland) Act

The Freedom of Information (Scotland) Act (FOI(S)A) 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 at: www.ico.gov.uk

FOI(S)A 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.

Moray Council Publication Scheme:-
http://www.moray.gov.uk/moray_standard/page_84996.html

Appendix 1

Moray Council Data Sharing Protocols

1.	Data sharing protocol between Aberdeen City Council, Aberdeenshire Council and The Moray Council re permanence panels Review of agency decisions following adoption and permanence panel of fostering panel recommendations	May 2012
2.	Memorandum of Understanding for the sharing of information	28 Feb 2011
3.	Information sharing protocol between Grampian Police and Aberdeen Council, Aberdeenshire Council and the Moray Council	
4.	Child Protection – Information Sharing Protocol between Aberdeen City Council, Aberdeenshire Council and The Moray Council	
5.	Joint Futures/Pan Grampian Partnership for Health and Social Care. General Protocol for the sharing of information to be supported by individual information sharing protocols – Adult Services between Aberdeen City Council, Aberdeenshire Council, The Moray Council and NHS Grampian	August 2004
6.	Pan Grampian General Protocol for the sharing of information (to be supported by Procedures and guidance documentation) Children and Young People Services	June 2005
7.	Anti-social behaviour (Scotland) Act 2004 – protocol for the sharing of information between The Moray Council, Grampian Police Force, The Reports Scottish Childrens' Reporters Administration (Moray Area), registers social landlords in Moray, Grampian Fire & Rescue Service, Victim Support Scotland, The Procurator Fiscal, Elgin	20 Dec 2007
8.	Multi-agency public protection arrangements to meet the requirements of the Management of Offenders (Scotland) Act 2005 (MAPPA) Memorandum of Understanding between the responsible authorities and the duty to co-operate agencies within the Grampian Area	16 Aug 2010
9.	Youth Justice – Information Sharing Protocol between Grampian Police and The Moray Council	3 July 2009
10.	Information sharing protocol for delayed discharge – Grampian	2009
11.	Adults at risk of harm – information sharing protocol between Aberdeen City Council, Aberdeenshire Council and The Moray Council, Grampian Police and NHS Grampian	01 May 2012
12.	Data sharing agreement – undertaking for supply of data between Skills Development Scotland Co Limited and the Moray Council	2011
13.	Protocol for the sharing of information in respect of Disclosure Scotland non-exempt childcare positions – information sharing protocol between Grampian Police, Aberdeen City Council, Aberdeenshire Council and The Moray Council	24 June 2008
14.	Provision of Information in connection with Licensing between Grampian Police, Licensing Boards & LSOs in Aberdeenshire, Aberdeen City and Moray Council areas	