Information Sharing Policy

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Data Sharing Policy

Key Messages

Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.

The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the Data Protection Act 1998 and the Information Governance Assurance Programme.

It is important that we protect and safeguard person-identifiable information that it gathers, creates processes and discloses, in order to comply with the law and to provide assurance to the public.

The Data Protection Act places a duty on all employees to protect personal information they may come into contact with during the course of their work.

In May 2011, the Information Commissioner issued a data sharing code of practice specifying that “under the right circumstances, and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service …. but…. rights under the Data Protection Act must be respected. Organisations that don’t understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness.”

Information can relate to staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, and must not be stored on removable or mobile media unless it is encrypted. Other alternatives to removable media should be chosen when sharing personal information.

Policy Detail

The aim of this policy is to:

- Provide a framework to:

  - Enable the legitimate sharing of data between staff, departments and other agencies.
  - Provide information to deliver better services.
  - To prevent and detect crime.
  - Consider the controls needed for information sharing.
  - Ensure the expected standards are met (including that partners to information sharing are aware of the obligations of consent or how to take appropriate account of an individual's objection).

- Establish a mechanism for the exchange of information between council departments, and the councils and other organisations.

Sharing Information

This policy covers two main types of information sharing:

- Systematic, routine information sharing where the same data sets are shared between the same organisations for an established purpose; and

- Exceptional, one-off decisions to share information for any of a range of purposes.

Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to one-off decisions about sharing.

Systematic information sharing - This will generally involve routine sharing of data sets between departments and/or organisations for an agreed purpose. It could also involve a group of departments and/or organisations making an arrangement to 'pool' their data for specific purposes.

Ad hoc or 'one-off' information sharing - much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information 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.

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both), you should consider what is the sharing meant to achieve? There should be a clear objective, or set of objectives. Please use the checklist at appendix 1.

In all circumstances of information sharing, staff will ensure that:

- When information needs to be shared, sharing complies with the law, guidance and best practice.

- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it.

- Individuals' rights will be respected, particularly confidentiality and security.

- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

Information Sharing Agreements

Information sharing agreements – sometimes known as 'Information or data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in an information 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.

An information sharing agreement must, at least, document the following:

- The purpose, or purposes, of the sharing.
- The legal basis for sharing.
- The potential recipients or types of recipient and the circumstances in which they will have access.
- Who the data controller(s) is and any data processor(s).
- The data to be shared.
- Data quality – accuracy, relevance, usability.
- 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; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected.
- Sanctions for failure to comply with the agreement or breaches by individual staff.

Privacy Impact Assessment

Before entering into any data sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or

potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on privacy impact assessments can be sought from the Information Commissioners website.

Further advice

With information sharing there will always be exceptional and difficult circumstances where advice may be needed. If you require assistance please contact your data Protection Officer or your legal team.

Further information can also be found in the ICO Data Sharing Code of Practice:

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

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Data Sharing Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
15/10/2015	Dave Randall Matthew Archer	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review

Appendix One

Checklist for Appendix Two:

You must work through the checklist below and record the required information and the decision on the form at appendix two, this will help you make a sound decision by requiring you to consider relevant factors.

Systematic Data Sharing:

Is the sharing justified – what is the sharing meant to achieve, what are the risks, is sharing proportionate to the issue and could the objective be achieved without sharing personal data?

Do you have the power to share – have you identified the relevant functions or powers, the nature of the information that you are being asked to share and any legal obligation (for example a statutory requirement or a court order)?

If you decide to share – what information needs to be shared, with whom and what security measures are in place to protect the information?

One Off Data Sharing:

Is the sharing justified – do you think you should share the information, what are the risks to the individual and to society, is an individual at risk of harm, do you need to consider an exemption in the DPA to share?

Do you have the power to share – have you identified the relevant functions or powers, the nature of the information that you are being asked to share and any legal obligation (for example a statutory requirement or a court order)?

If you decide to share? – what information needs to be shared, with whom and what security measures are in place to protect the information, ensure you give it to the right person

Full details can be found on the ICO Data Sharing checklist:

https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf

Appendix Two

Data Sharing Request Form	
Name of Organisation requesting shared data:	
Name and Position of person requesting data:	
Date of Request:	
Reference to Data Sharing Agreement (*if applicable)*	
Data Requested:	
Purpose:	

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.*	**YES** **NO**
What information needs to be shared? *You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "Use the minimum necessary personal confidential data ".*	
Who requires access to the shared personal data? *You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.*	
When will 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 will it be shared? *This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.*	
How will you 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.*	

How will individuals be made aware of the information sharing? *Consider what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the information held once shared?*	
What risk to the individual and/or the organisation 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?*	
Date Required by:	

Submitted By	
Name:	
Job Title:	
Date:	

Decision By	
Decision *Reason for disclosure or non-disclosure:*	
Name:	
Job Title:	
Date:	

Admin	
Date Data Disclosed:	