



# Information Sharing Policy

<b>Created by</b>	Stephen Berry
<b>Date</b>	16 <sup>th</sup> January 2013
<b>Reviewed by</b>	Tracy McKim
<b>Date</b>	20 <sup>th</sup> Jan 2015

## Document Control

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Notes / changes</b>
V1.0	21/6/2013	Mark Bleazard	Changes following Scrutiny meeting, approved by CM (live)
V1.1	20/1/2015	Tracy McKim	Migration to sharepoint new intranet
V1.2	16/11/2015	Tracy McKim	Change of service area

# Table of Contents

Golden Rules .....	3
1. Background and Purpose .....	4
2. Key Legislation.....	4
3. Scope.....	5
4. Definitions .....	5
5. Sharing Non-Personal Information .....	5
6. Sharing Personal Information .....	5
6.1 <i>Considerations before Sharing Personal Information</i> .....	5
6.2 <i>Conditions for Sharing Personal Information</i> .....	6
Consent.....	6
Legal Justification.....	6
Other Legislation .....	6
Sensitive Personal Information.....	6
6.3 <i>Consent</i> .....	7
6.4 <i>Regular or Ad hoc Sharing</i> .....	7
Regular .....	7
Ad Hoc .....	8
6.5 <i>Security Considerations</i> .....	8
7. Secondary Uses.....	9
8. Responsibilities .....	9
9. Legal Requirements .....	9
10. Termination of Employment.....	9
11. Further Help .....	9
Appendix A – Capacity to give Consent Guidance.....	10
Appendix B – Members Information Sharing Examples .....	13

## Golden Rules

The following are the key rules / messages from this policy, however these points do not replace the full policy which you should familiarise yourself with.

- The default position should always be safe and lawful sharing of information rather than not sharing
- Only the minimum amount of information necessary should be shared
- Information should be held securely and protected against inappropriate disclosure
- Consent from the service user should be obtained before any person identifiable information is shared with any external organisations or unrelated area of the Council unless sufficient legal powers allow otherwise. This includes personal information provided to Members where consent should be gained prior to sharing with other Members or council employees – see examples in Appendix B
- Regular sharing of information with external organisations should be supported by the development of an Information Sharing Protocol (ISP) in line with the Wales Accord on Sharing of Personal Information.
- Any sharing of information should adhere to the current security policies already in place
- Caution should be exercised when sharing information, but should not prevent information being shared in an emergency situation
- If specific guidance is required please contact a member of the Information Management team in People and Business Change
- Information should not be shared for a secondary purpose unless specific conditions are met

# 1. Background and Purpose

As a local authority we collect, store, process, share and dispose a vast amount of information as part of our duties. It is essential that this information is handled in such a way as to be compliant with both legislation and best practice, one such compliance requirement is sharing information safely and appropriately.

Information sharing is key to joined up service delivery. The Wales Accord on the Sharing of Personal Information (WASPI) was developed as a practical approach to multi agency sharing for the public sector in Wales, and Newport signed up to this in January 2011.

Information sharing can bring many benefits. It can support more efficient, easier to access services and also help to ensure cooperation between organisations to deliver services. However, sharing information also presents risks especially as computer systems become more complex and their use more widespread. There is more potential for information about our lives, possibly highly sensitive, to become known to more and more people.

The purpose of this policy is to inform staff of their responsibilities and give guidance regarding the sharing of information.

The benefits of this policy are as follows:-

- Enables the council to meet statutory and good practice requirements
- Ensures that staff have appropriate guidance relating to information sharing
- Ensures that information is shared appropriately and safely
- Supports the protection of service users' rights
- Facilitates effective service delivery
- Reduces the risk of being issued with considerable financial penalties by the Information Commissioner's Office (ICO) for sharing information inappropriately

# 2. Key Legislation

The [Data Protection Act 1998](#) establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the rights of individuals to respect for the privacy of their personal details.

### 3. Scope

This policy applies to information held in any format (paper or electronic media as the Data Protection Act defines) for the purposes of delivering Council services.

It applies to all employees, Members and any other parties who access and maintain records on behalf of the council.

### 4. Definitions

Definitions relating to information sharing are as follows:

- Personal information – information that could directly, or in conjunction with other available information, identify an individual
- Consent - 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 – definition from the European Data Protection Directive
- WASPI - the **Wales Accord on the Sharing of Personal Information (WASPI)** provides a framework for service-providing organisations directly concerned with the health, education, safety, crime prevention and social wellbeing of people in Wales. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others in a lawful and intelligent way.
- Information Sharing Protocol (ISP) – an agreement that sets out the lawful basis for the use of personal information by the public sector, across traditional organisational boundaries, to achieve better policies and deliver better services for individuals and society as a whole.

### 5. Sharing Non-Personal Information

There are no real restrictions surrounding the sharing of non-personal information. However, officers should consider any risks involved depending on the nature of the information.

### 6. Sharing Personal Information

#### 6.1 *Considerations before Sharing Personal Information*

Before sharing information you should consider:

- Why you need to share personal information?
- Do you need to share information in a personally identifiable form or would anonymised or statistical information be enough?
- What legal provisions exist that require or permit you to share information?
- Might any issues arise as the result of sharing confidential or sensitive information?
- Is consent from the individual required, and if so how would you obtain consent? What would you do if consent is withheld?
- Who is the information being shared with? Have they got a legitimate right to be given the information?
- What are the benefits to the service user and the council in sharing and how do they compare with any risks or disadvantages?

## **6.2 Conditions for Sharing Personal Information**

The Data Protection Act stipulates a number of conditions that must be met before the sharing of personal information can take place. Namely :

### **Consent**

Generally information sharing requires some form of consent from the individual the information relates to (or their legal representative), and they must be provided with adequate information to enable them to make an informed decision. [For further details on consent please refer to Section 6.3.](#)

### **Legal Justification**

When sharing personal information without consent, there must be legal justification to do so. Such situations where information might be shared without consent include:

- 'Life and death' situations, for example, where information is shared in an emergency in order to preserve life;
- where a person's condition indicates they may be a risk to the public or may inflict self-harm;
- in order to prevent abuse or serious harm to others;
- on a case-by-case basis, to prevent serious crime and support detection, investigation and punishment of serious crime.

This is not an exhaustive list and each situation should be considered on a case by case basis.

### **Other Legislation**

In addition to legislation about information sharing, there are a large number of specific acts of Parliament that give a duty or power to share, or not to share, information about children and young people for various purposes. Advice should be sought on these matters before deciding whether to share information.

### **Sensitive Personal Information**

The Data Protection Act also highlights that when sharing sensitive personal information, it must be treated with greater care. **In these cases please refer to the Information Management team for advice prior to sharing.**

Sensitive personal information is information relating to:

- Race or ethnic origin
- Political views
- Religious beliefs
- Trade Union Membership
- Physical or Mental Health condition
- Sexual life
- Commission, or alleged commission, of them of any offence
- Any proceedings for any offence committed/alleged

### **6.3 Consent**

Consent to disclose information may be explicit or implied. This consent should be informed and freely given. Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual'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".

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a customer's failure to return a form or respond to a leaflet.

#### Implied Consent

This is deemed to be agreement that has been signalled by behaviour or actions of an informed service user. In order for implied consent to be valid it is important that service users are made aware that information about them will be shared, who with and of the service user's right to refuse this. In addition to information provided to service users during conversations leaflets, posters and letters can play a useful part in conveying to service users the necessity of information sharing and the benefits it offers.

#### Explicit Consent

This is a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where options and consequences have been made clear to the service user. Explicit consent is the ideal as no questions can be raised as to what the agreement was.

#### Refused Consent

Where a service user has refused to share information this should be recorded in their service record and time stamped. That information must NOT be shared from that point on (unless legal requirements or an overriding public interest dictate otherwise). The service user should be made aware that any previously information that has been shared will not be recoverable.

#### Capacity to give Consent

The circumstances where a Service User is deemed to have capacity to give consent can vary and be dependent on a number of factors. For further information on this please refer to Appendix A.

### **6.4 Regular or Ad hoc Sharing**

Consideration must be given to whether the sharing of information is likely to be a regular occurrence or a "one-off" (ad hoc) instance.

#### **Regular**

An example of regular sharing is where personal information is routinely shared between the Council and a partner organisation, for instance personal information relating to housing needs may be passed between ourselves and registered social landlords such as Newport City Homes.

All staff that regularly share personal identifiable information must ensure that an Information Sharing Protocol exists before sharing any information with non-Newport City Council organisations.

In January 2011 Newport City Council signed the Wales Accord for the Sharing of Personal Information (WASPI). By signing the Accord, it has agreed to:

- Work to a common approach for the sharing of personal information with other public and voluntary sector organisations
- Develop supporting local Information Sharing Protocols (ISP) using the WASPI template and guidance
- Raise staff awareness of information sharing responsibilities

Staff should ensure that any new or reviewed information sharing protocols are developed in line with the WASPI guidance – to do this please contact the Information Management team in the first instance where the WASPI trained ISP Facilitator will provide advice and guidance throughout the local development process of an ISP.

## **Ad Hoc**

An example of “ad hoc” sharing is where information needs to be shared where there is no routine agreement in place, sometimes involving conditions of real urgency or emergency situations.

Where the need for ad hoc sharing arises, staff must exercise their professional judgement to determine whether the information should be shared. Staff must consider their responsibility in relation to the Data Protection Act and any professional guidance or ethical rules that are likely to be relevant to the type of decisions about disclosing personal information 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 staff should record the sharing as soon as possible, detailing the circumstances, the information shared and reasons for disclosure.

If unsure whether to share information, staff should err on the side of caution and seek guidance from the Information Management Team before proceeding. In the event of an emergency, obtaining this guidance may not be practical in which case staff should proceed whilst exercising their judgement in accordance with the advice stated elsewhere in this policy.

## **6.5 Security Considerations**

When sharing personal information, consideration should be given to ensure that the methods of transfer are secure and adhere to Newport City Council’s security policies.

Of particular note, Secure Email should be used where possible to transfer information to an external organisation. Where the recipient does not have access to Secure Email the security of the alternative transfer method should be carefully considered. As a minimal requirement, personal information sent by email must be sent as a password-protected attachment with the password disclosed in a separate email or telephone call.

The Council is currently developing a solution utilising the Juniper IVE software which will enable the secure transfer of information to anyone with Internet Access. Please contact the Information Management team if you feel you have a need to utilise this.

## 7. Secondary Uses

The Data Protection Act states that we cannot share personal information for purposes other than those for which it was obtained. For example, under the Data Protection Act, leisure centres could not request details from Social Services of service users in order to target them for marketing information as the information was not given to Social Services for this reason. Similarly, a Member should not request, or be provided, personal information from an area of the council they are not directly involved in.

However, we can disclose personal information if one of the following criteria has been met:

- It has been effectively anonymised (see Appendix A)
- It is required by law
- The service user has given explicit consent
- Staff are satisfied that the legal and professional criteria for disclosure without consent in the 'public interest' have been met and have sought advice in the case of any doubt.

## 8. Responsibilities

All Councillors and employees of the Council are responsible for adhering to this policy when sharing personal or sensitive information.

It is also the responsibility of officers to ensure that any third-parties involved in the information sharing process are aware of the terms and conditions contained within this policy.

Failure to do so may result in action in accordance with the Council's [Disciplinary Policy](#) / [Members' Code of Conduct](#).

## 9. Legal Requirements

The Council has a duty to comply with all legislation, including (but not exclusively):

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

## 10. Termination of Employment

Line managers of departing or transferring staff must give consideration to any information sharing issues arising from staff changes. The [termination checklist](#) for managers may be useful.

## 11. Further Help

For further advice and assistance on any of the issues covered by this policy, please contact the Information Management team. Contact details are available on the [Information Management Intranet page](#).

## Appendix A – Capacity to give Consent Guidance

### 1. Capacity To Give Consent

All people aged 16 are presumed, in law, to have the capacity to give or withhold their consent to disclosure of confidential information unless there is evidence to the contrary. A service user who is suffering from a mental disorder or impairment does not necessarily lack the capacity to give or withhold their consent. Equally, service users who would otherwise be competent may be temporarily incapable of giving valid consent due to factors such as extreme fatigue, drunkenness, shock, fear, severe pain or sedation. The fact that an individual has made a decision that appears to others to be irrational or unjustified should not be taken on its own as conclusive evidence that the individual lacks mental capacity to make that decision. If, however, the decision is clearly contrary to previously expressed wishes, or is based on a misperception of reality, this may be indicative of a lack of capacity and further investigation will be required.

#### Young Persons

There is no presumption of capacity for people under 16 in England and Wales and those under this age must demonstrate their competence by meeting certain standards set by the courts. The central test is whether the young person has sufficient understanding and intelligence to understand fully what is proposed.

To demonstrate capacity individuals should be able to:-

- Understand in simple language (with use of communication aids if appropriate) what is to be disclosed and why it is being disclosed.
- Understand the main benefits of disclosure
- Understand, in broad terms, the consequences of disclosure
- Retain the information long enough to use it and weigh it in the balance in order to arrive at a decision.
- Communicate the decision
- Make a free choice

When assessing a child's capacity it is important to explain the issues in a way that is suitable for their age. If the child is competent to understand what is involved in any proposals then their wishes should be respected unless compelling reasons to not do so (such as suspicions of abuse) exist. Every reasonable effort must be made to persuade the child to involve parents or guardians, particularly for important or life-changing decisions.

#### Mental Capacity

Individuals with mental disorders or learning disabilities should not automatically be regarded as lacking the capacity to give or withhold their consent to disclosure of information. Unless unconscious, most people suffering from a mental impairment can make valid decisions about some matters that affect them. An individual's mental capacity must be judged in relation to that particular decision being made. If a service user has the requisite capacity, disclosure of information to relatives or third parties requires Service User consent. If there is ever doubt over an individual's competence to give or withhold consent then a second opinion should be sought.

## **2. Welfare Attorney**

In England and Wales, the Mental Capacity Act 2005 allows people over 18 year of age who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Protection may also appoint a deputy to make these decisions. Where a service user lacks capacity and has no relatives or friends to be consulted, the Mental Capacity Act requires an Independent Mental Capacity Advocate to be appointed and consulted about all decisions about “serious medical treatment”, or place of residence. An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs.

## **3. Risk Of Abuse or Neglect**

Where staff have concerns about a service user lacking capacity who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information given promptly to an appropriate person or statutory body, in order to prevent further harm. Where there is any doubt as to whether disclosure is considered to be in a service user’s best interests it is recommended that staff discuss the matter on an anonymised basis with a senior colleague, Data Protection Officer or similar. All discussions, along with concerns and any actions, or intended actions, are recorded in the service user’s records.

## **4. Parental Consent**

Anyone with parental responsibility can give or withhold consent to the release of information where the child lacks capacity. Not all parents have parental responsibility.

- In relation to children born after 1<sup>st</sup> December 2003, both of a child’s biological parents have parental responsibility if they are registered on a child’s birth certificate.
- In relation to children born before this date, a child’s biological father will only automatically acquire parental responsibility if the parents were married at the time of the child’s birth or some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement. Neither parent loses parental responsibility on divorce.
- Where the child has been formally adopted, the adoptive parents are the child’s legal parents and automatically acquire parental responsibility.
- Where the child has been born as a result of assisted reproduction, there are rules under the Human Fertilisation and Embryology Act 2008 that determine the child’s legal parentage.
- In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court.
- A local authority acquires parental responsibility (shared with the parents) while the child the subject of a care or supervision order.
- In some circumstances parental responsibility can be delegated to other carers such as grandparents and child minders.

If there is doubt about whether the person giving or withholding consent has parental responsibility, legal advice should be sought.

Where an individual who has parental responsibility refuses to share relevant information but it is determined that this would not be in the best interest of the child (for example, if it puts the child at risk of significant harm), disclosure may take place in the public interest without consent.

## **5. Concerns About Children**

Where staff have concerns about a child who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information given promptly to an appropriate person or statutory body, in order to prevent further harm. The best interests of the child or children involved must guide decision making at all times. Staff should not make promises to children about confidentiality that they may not be able to keep but, as in the case with any service user, trust is best maintained if disclosure is not made without prior discussion between the staff member and the child, unless to do so would expose the child or others to an increased risk of serious harm.

Where there is any doubt as to whether disclosure is in the child's best interest, it is recommended that the staff member discusses the matter anonymously with an experienced colleague, Safeguarding Children and Families Team or similar. Staff must ensure that their concerns, and the actions they have taken, or intend to take, including any discussion with the child, colleagues or professionals in other agencies, are clearly recorded in the service user's record.

## **6. Decisions Taken On Behalf of Someone**

All decisions taken on behalf of someone who lacks capacity must be taken in their best interest. A best interest judgement is not an attempt to determine what the service user would have wanted. It is as objective a test as possible of what would be in the service user's best interests, taking into account all relevant factors. A number of factors should be addressed including:

- The service user's own wishes (where they can be determined)
- Where there is more than one option, which option is least restrictive of the service user's future choices.
- The view of the parents, where the service user is a child.
- The views of people close to the service user. Especially close relatives, partners, carers, welfare attorneys, court-appointed deputies or guardians, about what the patient is likely to see as beneficial.

## Appendix B – Members Information Sharing Examples

Extract from Information Commissioner’s Guidance Data Protection Good Practice Note

<u>Example</u>	<u>Good Practice</u>	<u>Bad Practice</u>
An elected member helps a constituent with a particular issue and wishes to use the constituent’s personal information to progress a party political matter on the same issue.	The elected member seeks the consent of the constituent before using their personal information.	The elected member uses the constituent’s personal information without their consent.
A resident asks one of their elected members in a multi-member ward for help about teenagers acting in an intimidating way in the area. The elected member wishes to share the constituent’s complaint with the other members of the ward because it is an issue of general concern.	The elected member lets the constituent know that he wants to give the details of their complaint to the other ward councillors and why he wants to do that rather than giving a general description of the complaint to other ward members.  If the constituent objects, then his wishes are respected and only the general nature of the complaint is shared.	The elected member does not inform the constituent that they intend to give the details of their particular complaint to the other ward members and releases the information. The resident finds out and is afraid of reprisals if the information they have leaks out.
A resident asks one elected member for help with a noisy neighbour.	The member lets the resident know he intends to give their personal information to another ward member because that particular councillor has knowledge and experience with this subject. If the constituent objects, he does not disclose the information.	The elected member does not tell the complainant that he intends to give their personal information to another ward member and goes ahead anyway. The resident finds out and makes a complaint.