# Information Sharing Policy

~~??? 2020~~May 2022

## Table of Contents

## 1 Overview

Information sharing is key to West Lindsey District Council's ("the Council") goal of delivering better and more efficient services that are coordinated around the needs of the individual. Sharing information both internally and with our partners is essential to support early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection. Information sharing is a vital element in improving outcomes for all.

The Council understands that it is most important that people remain confident that we keep their personal information safe and secure and that staff maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that all staff are aware of how they can share information appropriately as part of their day-to-day responsibilities and do so confidently.

## 2 Purpose

The purpose of this policy is to:

- Provide a framework for the Council and those working on its behalf to:
    - Provide information to deliver better services;
    - Consider the controls needed for information sharing; and
    - Make sure that partners sharing information are aware of the Council's Minimum Security Standards for securing information; the obligations of consent; and how to take appropriate account of an individual's objection to the sharing.
- Establish a mechanism for the exchange of information between the Council and other organisations.

## 3 Scope

This Policy applies to all staff including those who are responsible for managing partnerships where information will be shared and those who are responsible for creating or providing the information that is to be shared.

Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations. Information sharing can be:

- 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; or
- Exceptional, one-off disclosures of data in unexpected or emergency situations.

**Sharing non-personal information with other organisations.** This is where the Council shares key information with other organisations to: improve customer experience; facilitate commissioning of services; manage and plan future services; assure and improve the quality of services; statutory returns and requests; to train staff; to audit performance.

**Sharing Personal information with other organisations.** As long as it is necessary and proportionate, the Council can share personal information with other organisations: to prevent crime; to investigate complaints or potential legal claims; to protect children and adults at risk; to assess need and service delivery.

This policy covers two main types of information sharing. These are explained in more detail in Para 4:

- "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.

# 4 Policy

## 4.1 Factors to consider before sharing information

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) staff must consider firstly whether there is a legal power either expressed or implied by legislation or an overriding public interest to share the data.

If staff are unsure about this they must seek advice from the Data Protection Officer ~~or the Information Governance Officer~~.

**Commented [JB1]:** Role no longer exists

If the answer to~~is~~ the above question is yes, staff must then consider what the sharing is meant to achieve and there should be a clear objective, or set of objectives. Being clear about this will identify the following:

- 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.
- 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 Data Protection principle states: adequate, relevant and limited to what is necessary in relation to the purposes for which they are

processed ('data minimisation')~~The third Data Protection principle states, "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."~~

- 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 should it be shared? 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.

- How do we make individuals aware of the information sharing? Consider what to tell the individuals concerned. Is their consent needed? Should the individuals be provided with a Privacy Notice, notifying them of who you are going to share their data with? 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?

In all circumstances of information sharing, staff will make sure that:

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

- The information must be processed lawfully and fairly to comply with the UK General Data Protection Regulation (GDPR) and the Data Protection Act ~~1998~~ 2018 (DPA). ~~-~~Also, ~~and~~ the ICO's Code of Practice on Data Sharing ~~published under section 52 of the DPA~~ must be followed. This Policy has been written in accordance with the Code ~~although~~ and further information ~~on the Code~~ can be found on the ICO's website www.ico.org.uk

- The sharing must not contravene other laws such as Article 8 of the Human Rights Act 1998 being The Right to Privacy.

**Commented [JB2]:** Updated to reflect the UK GDPR and DPA 2018

- 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 regarding the confidentiality and security of their personal information and the sharing must not contravene laws such as the Common Law of Confidentiality;
- Confidentiality will be maintained unless there is a robust public interest or a legal justification in disclosure; and
- They undertake reviews of information sharing to make sure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

### 4.2 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;
- Any particular obligations on all parties to the agreement, giving an assurance around the standards expected; and

- Sanctions for failure to comply with the agreement or breaches by individual staff.

### 4.3 Data Protection ~~Privacy~~ Impact Assessments

Commented [JB3]: Referred to as DPIA

Before entering into any information sharing arrangement, it is good practice to carry out a data protection ~~privacy~~ impact assessment (DPIA). 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, or causing distress or embarrassment 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 DPIAs~~privacy impact assessments~~ can be found on Minerva or on the ICOs website.

## 5 Policy Compliance

### 5.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements, such as those required by the ~~Data Protection Act 1998~~UK GDPR, DPA 2018, ~~and the~~ Freedom of Information Act 2000 and Environmental Information Regulations 2004, these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Corporate Policy and Resources Committee.

### 5.2 Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

Where personal information is being shared a breach of this Policy could result in a breach of the ~~Data Protection Act 1998~~UK GDPR/DPA 2018, for which the Council could face substantial fines, reputational damage and possible criminal sanctions.

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Council encourages the notification of Data Protection breaches by staff in accordance with the ~~Data Protection Breach Management Reprting Policy and Procedure~~Data Protection Breach Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

Commented [JB4]: Policy name updated

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer ~~or the Information Governance Officer~~.

### 5.3 Policy Review

This Policy will be reviewed every three years by the Corporate Information Governance Group and approved by the Corporate Policy and Resources Committee. Authority to approve interim updates may be delegated to the ~~Director of Resources in consultation with the~~ Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee as required.

## 6 Related Standards, Policies, and Processes

- Information Governance Policy
- Legal Responsibilities Policy
- Data Protection Policy
- Data Quality Policy
- ~~Data Protection Breach Reporting Policy and Procedure~~Data Protection Breach Policy
- Freedom of Information Policy & Environmental Information Regulations Policy
- Records Management Policy
- Information Security Policy
- Staff Code of Conduct
- Member's Code of Conduct
- Retention and Disposal Policy

## 7 Definitions

| | |
|---|---|
| Data Sharing | 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. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes. |
| Data Controller | A data controller is the "person" recognised in law (i.e. an individual; organisation; or other corporate and unincorporated body of persons) who determines the purposes and means of processing personal data~~determines the purposes for which and the manner in which any personal data are, or are to be, processed~~. |

**Commented [JB5]:** Amended as per ICO wording.

| | |
|---|---|
| Data Processor | Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. |
| Data Sharing Agreements | Set out a common set of rules to be adopted by various organisations involved in a data sharing operation. |
| Data Protection ~~Privacy~~ Impact Assessments | A formalised document which shows the possible threats to privacy which could arise from a business activity. |
| Data Quality | Data quality relates to the accuracy, validity, reliability, timeliness, relevance and completeness of data and information. |
| Data Security | The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity and availability of information. |
| Information | *"Information is data imbued with meaning and purpose". Anon*<br><br>Information is something which tells us something and can also be communicated to someone else in a meaningful way. Information is data that is put into context, can be comprehended, understood and shared with other people and / or machines. |
| Retention | Means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period. |
| ICO-Information Commissioner's Office | The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk |

| | |
|---|---|
| Personal Data | ~~Defined in s(1) of the DPA, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the Council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual. At least one of the conditions in Schedule 2 to the DPA must be met to process personal data.~~ Personal data is information that relates to an identified or identifiable individual. |
| Processing | Covers a broad range of activities such that virtually any use of personal information or data will amount to processing. |
| ~~Processed fairly and lawfully~~ | ~~Data must be processed in accordance with the 3 provisions of the DPA. These are the data protection principles, the rights of the individual, and notification.~~ |
| Privacy Notice | ~~As a minimum,~~GDPR sets out what information must be included in a Privacy Notice. It must ~~should~~ tell people who you are, what you are going to do with their information and who~~w~~ it will be shared with. ~~However it can also tell people more than this. It can for example~~it must also provide information about people's rights of access to their data ~~or~~ and your arrangements for keeping their data secure. ~~Whatever you include in your Notice,~~ I~~i~~ts primary purpose is to make sure that information is collected and used fairly. |

**Commented [JB6]:** Updated to comply with UK GDPR

**Commented [JB7]:** No requirement to include

**Commented [JB8]:** Updated to comply with UK GDPR

## Appendix 1 – Flowchart of Key Questions for Information Sharing