Data Sharing Guidance

Author: Rachel Everitt

Date: September 2024

Version: v0.2

Title	**Data Sharing Guidance**
Author	**Information Governance Manager and Data Protection Officer**
Owner	**Data Protection Officer**
Created	**March 2022**
Approved by	**Audit Committee**
Date of Approval	**February 2025**
Review Date	**February 2027**

Document Version Control

Document Version Control	
Issue Number	Date
0.01	March 2022
0.02	September 2024

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Background

The Information Commissioner has published a Data Sharing Code of Practice which provides a framework for organisations to make good quality decisions about data sharing.

Information rights are high on the public agenda. Citizens' and consumers' rights under the Data Protection Act 2018 (DPA) and the implications of General Data Protection Regulation (UKGDPR) must be respected along with their rights to confidentiality under the Common Law of Confidentiality and their rights under the Human Rights Act 1998. Unlawful disclosure of an individual's personal data can have serious implications to that individual. We want citizens and consumers to be able to benefit from the responsible sharing of information, confident that their personal data is being handled responsibly and securely.

People want their personal data to work for them. They expect organisations to share their personal data where it is necessary to provide them with the service they want. However, they do expect an appropriate level of choice and control, especially over their sensitive data.

The following information provided within this Corporate Guide provides the necessary tools and advice for sharing personal data between services and with outside organisations.

Attached at Appendix A are the 7 'golden rules' for sharing data which must be adhered to at all times.

2. Introduction

Data Sharing – Personal Information

We are increasingly encouraged to provide efficient, effective services by working more closely within our own organisation and with other bodies whether these are public, private or third sector organisations. By joining up our information resources, we can deliver a better service to the public. Often, this involves sharing personal information about individuals.

The Data Protection Act and UKGDPR exist to regulate the processing of personal data including the obtaining, holding and disclosure of such data and by adhering to its principles we can ensure that we can share personal information, without compromising the rights of individuals. This guidance provides you with a clearly defined framework within which personal information can be shared fairly and lawfully.

What do we mean by Personal Data?

Data which relates to a living individual who can be identified –

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. For example, if we can put a payroll number and name together, we have personal data.

What do we mean by Sensitive Personal Data?

UKGDPR guidance defines Personal Sensitive Data consisting of information related to:

- Race
- Ethnic origin
- Politics
- Religion;
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation.

Processing of Personal & Personal Sensitive Data

UKGDPR requires that, in the first instance, you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under Article 6 and to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.

Before any personal data is 'processed', which includes where it is obtained, held, recorded or disclosed, for whatever reason, you must make sure that you have legitimate grounds for collecting and using the personal data in the first place, the individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice and will require consent from the individual supplying details about themselves to receive specific services.

There are 8 prescribed data protection principles with which we must ensure we comply with when processing individual personal data, these principles can be found at Appendix B. The first principle says that personal data shall be "processed fairly and lawfully" and shall not be processed unless at least one of these Conditions is met and, in the case of Sensitive Personal data, at least one of the additional Conditions set out in the guidance is met.

In summary, "personal data shall be processed fairly and lawfully" means:

- That you must have legitimate grounds for collecting and using the personal data
- That you do not use the data in ways that have unjustified adverse effects on the individuals concerned
- That you are transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data.
- That you handle people's personal data only in ways they would reasonably expect; and
- That you make sure you do not do anything unlawful with the data.

The lawful bases for processing are set out in Article 6 of the UKGDPR. At least one of these must apply whenever you process personal data, these are:

- **Consent** - The individual who the personal data is about has consented to the processing?
- **Contract** - 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
- **Legal Obligation** - The processing is necessary because of a legal requirement that applies to you.
- **Vital Interests** - The processing is necessary to protect the individuals "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 for a serious health matter.
- **Public task** - The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests** - the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. The decision to disclose under this condition will need to be fully justified.

When processing Sensitive Personal Data a further set of conditions must also be met, namely:

- The individual who the sensitive personal data is about has given explicit consent to the processing
- The processing is necessary so that you can comply with employment law
- The processing is necessary to protect the vital interests of:
    - The individual
    - Another person
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents.
- The individual has deliberately made the information public.

- The processing is necessary for administering justice, or for exercising statutory or government functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Disclosing or sharing of Personal & Personal Sensitive Data?

If you are asked to disclose or share information, you must follow these steps in this order:

1. Do you have the Power to have the information disclosed to you?

   You must be satisfied that the Council and therefore your service has the necessary power to disclose or share the information sought, either from a specific power or where it is felt that disclosure is reasonably incidental to that power or can be implied. Refer to the Acts/Regulations list provided within Part 2 of the "Request for the Sharing of Personal Data between Services" Form at Appendix D.

   Once the power to disclose the information has been identified?

2. Are you complying with the UKGDPR/Data Protection Principles and Conditions?

   You need to ensure that in disclosing or sharing the information, you are complying with the UKGDPR/Data Protection Principles set out in paragraph 2.4, above.

   If you are not complying with these requirements?

3. What Exemption are you using to have information disclosed?

   Exemptions from the UKGDPR's transparency obligations and individual rights are permissible, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure to safeguard:

   - National security; defence;

- Public security;
- The prevention, investigation, detection or prosecution of criminal offences;
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- The protection of judicial independence and proceedings;
    - Breaches of ethics in regulated professions; monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others;
- The enforcement of civil law matters.

If none of these apply, then in certain circumstances a breach of the Data Protection Act may be defensible and you may still disclose information under special circumstances e.g. to prevent harm. Therefore have you some other reason to disclose or share the information?

4. <u>It is extremely important that the information is disclosed immediately to prevent e.g. harm to a child or adult – "Reasonable Cause"</u>
   A judgement has been made to disclose personal data because it is within the "public interest" to do so, and it is reasonable, proportionate and necessary. This may be because you have reasonable cause to believe that harm may come to a child or adult or similar. Although this may still mean there is a breach of UKGDPR/DPA, this may be defensible in the circumstances. To prevent any unnecessary delays disclosure must be immediate and therefore it is not necessary to complete the Data Sharing Form at Appendix D. Please though ensure you have a clear record detailing why you have requested personal information to be disclosed or have disclosed personal date under "Reasonable Cause" as this will help if you are required to defend this decision.

   Attached at Appendix A and C are some useful reference guides which you should use to help when a decision to disclose has to be made. Consideration

should also be given as to whether there may be any breach of confidence and/or human rights.

Request to share personal data between services "disclosure of personal data" application form

Attached at Appendix D is the Council's internal "Request for the Disclosure of Personal Data" application form which must be completed in all cases where personal data is being requested by another service, except if personal data is shared under "Reasonable Cause" see 2.5 (3) above, where data needs to be exchanged as a matter of urgency.

Sharing of data externally between partners/organisations

Before entering into any Data Sharing initiative between partners/other organisations it is mandatory to undertake a Privacy Impact Assessment (PIA). A Privacy Impact Assessment will help to understand the risks associated with sharing the personal/personal sensitive data being considered.

A PIA needs to be actively engaged with and completed from the outset by all organisations involved in the data sharing proposal, so all organisations involved understand the implications of sharing the data they are responsible for. Once complete the PIA will provide a very useful reference document for drawing up a detailed Information Sharing Agreement.

Developing an Information Sharing Agreement

What is an Information Sharing Agreement?

An Information Sharing Agreement is effectively an agreed set of rules and conditions that give important information about why, how and with whom personal information will be shared and how this sharing will comply with the legislation that is there to protect an individuals personal data, namely the Data Protection Act, Human Rights Act and the Common Law of Confidentiality. The Information Sharing Agreement once complete makes it clear what each organisation/department involved in the sharing has signed up to in order to meet these requirements.

When are Information Sharing Agreements necessary?

Information Sharing Agreements are created when a number of partners (which might be agencies, organisations from the public, private or voluntary sectors or services such as between departments within the same organisation) wish to better make use of their customers'/clients' personal data to improve services.

If you intend to share personal data with another body/another part of the organisation and/or there is a new purpose for which you wish to use personal data, the arrangements will need to be formalised in an Information Sharing Agreement.

For further information about data sharing refer to the latest ICO Data Sharing Code of Practice which can be found on the ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/ or on Bury Council's Intranet. Also available is an Information Sharing and Management Toolkit to help organisations better understand and develop data sharing arrangements between organisations which can be accessed through this link: http://informationsharing.co.uk/.

Data Controllers and Data Processors – Sharing & Processing Data?

There is a clear distinction between organisations that share personal data within or between themselves and organisations that require personal data to be processed on their behalf. Both types of sharing of personal data require the establishment of either an Information Sharing Agreement or an Information Processing Agreement examples of which can be found on the Data Protection Intranet web pages.

Data Controllers

Data sharing is defined by the ICO where two or more organisations agree to share data between themselves and each organisation determines the purpose for which and the manner in which the personal data is processed. They are responsible for the way in which the data they share and receive is managed. They are known as the Data Controllers.

Data Processors

These occur when a Data Controller shares data with another party that processes personal data on its behalf. These organisations are known as Data Processors. A data processor would be an organisation which obtain, records or holds information/data on behalf of the Data Controller.

When a Data Controller uses a data processor the DPA advice and guidance requires that a Data Controller draws up a written contract (Information Processing Agreement) that clearly states that the data processor only acts on instructions from the data controller and that the data processor has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle "Information Security" – Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A Data Processor involved in Data Sharing does not have any direct Data Protection responsibilities of its own; they are all imposed on it through its contract (Information Processing Agreement) with the Data Controller.

Summary

This guidance has been written to assist in the preparation of Data Sharing Initiatives internally between services and externally between partners. Further guidance can be obtained from the Information Commissioners Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

Appendix A: 7 Golden Rules for Data Sharing

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden where an exemption applies or there is reasonable cause as it is in the public interest. You will need to base your judgement on the facts of the case.

5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix B: Eight prescribed Data Protection Principles

These principles require personal data to be:

1. Processed (defined to included 'obtained') fairly and lawfully

2. Obtained only for specified and lawful purposes and not processed incompatibly with the specified purposes;

3. Adequate, relevant, and not excessive for their purpose;

4. Accurate and up to date;

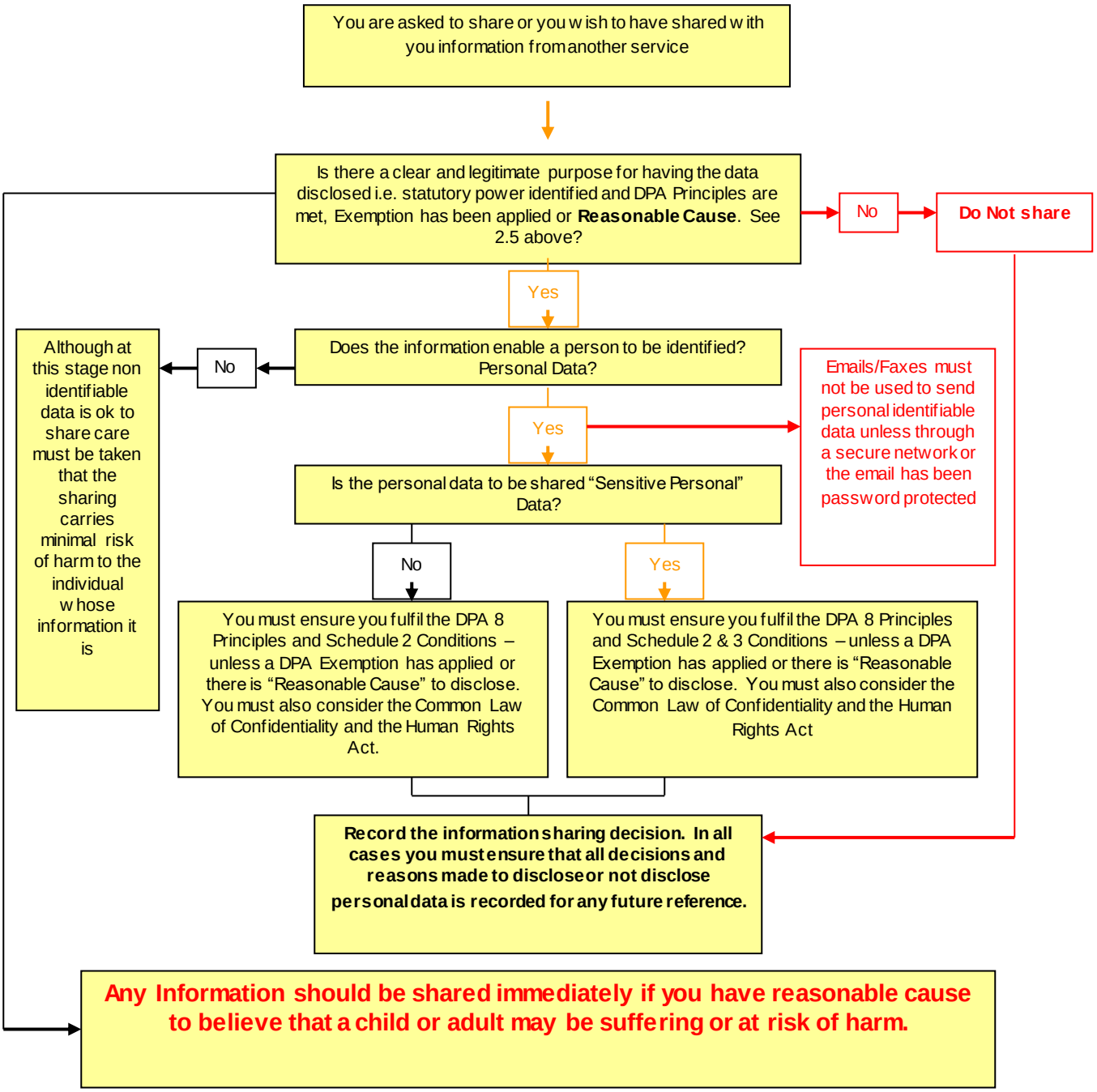
5. Not kept for longer than necessary;

6. Processed in accordance with the rights of data subjects;

7. Secure against unauthorised or unlawful processing;

8. Not transferred to a country outside of the European Economic Association (EEA) where the is inadequate protection for the data in that country.

Appendix C: Flowchart of key questions for Internal information sharing



Appendix D: Request for the disclosure/sharing or disclosure of personal data between services

(Note: A separate form must be completed for each disclosure request)

Officer Name:	
Service	
Full Address	
Telephone Number	
Email Address	
Investigation/Operation Name (if applicable)	
Date	

Details of Application

1. Provide details of where the information is held?	
Service holding the information:	
Service Address:	
Contact Name:	
Telephone Number:	
1. Describe the information you are requesting to be disclosed or are	

2. Please confirm the Act/Regulation that provides or implies the power to provide the information.

☐ **Crime & Disorder Act 1998 (Section 115)**
(the information must be necessary for the detection or prevention of crime or disorder)

☐ **Children Act 1989 (Section 27)**
(the information is required to assist with the duty to safeguard and promote the welfare of children or to prevent them suffering harm))

☐ **Regulation 2d of the Child Support (Information, Evidence and Disclosure) Regulations 1992**
(the information is required to enable an application for maintenance to be determined)

☐ **Regulation 4 Council Tax (Administration & Enforcement) Regulations 1992**
(the information is required for Council Tax functions)

☐ **Social Security Administration Act 1992 (Section 122E / Social Security Administration (Fraud) Act 1997 (Section 2)**
(the information is required by another local authority for investigating offences or checking accuracy of information relating to housing or council tax benefit)

☐ **Social Security Administration Act 1992 (Section 122D) / Social Security Administration (Fraud) Act 1997 (Section 2)**
(the information is required by a social security government department for investigating offences or checking accuracy of information relating to housing or council tax benefit))

☐ **The Learning and Skills Act 2000 (Section 120)**
(the information is required to assist with the provision of services to young people under this Act)

☐ **Local Government Finance Act 1992 (Section 27)**
(the information relates to property and is required to assist with Customs & Excise functions)

☐ **Tax Credits Act 1999 (Paragraph 5 of Schedule 5)**
(the information is required for purposes relating to tax credit)

☐ **The Housing Act 1996 (Section 213 – duty to co-operate)**

(the information is required by another local authority to assist with homelessness functions under this Act)

☐ **Building Act 1984 (Section 77)**

(the information must be required in order to identify the owner of a dangerous building or structure so a section 77 order can be served on them)

☐ **Building Act 1984 (Section 78)**

(the information must be required in order to identify the owner/occupier* of a dangerous building or structure so a section 78 notice can be served on them*/expenses incurred under this section can be recovered* (*delete as applicable))*

☐ **Building Act 1984 (Section 79)**

(the information must be required in order to identify the owner of a seriously dilapidated building or structure so a section 79 notice can be served on them)

☐ **Other?** Please provide details of the Act/Regulation that provides or implies the power to provide the information.

3. By requesting for this information to be disclosed are you complying with the DPA 8 Prescribed Principles and Schedule 2 Conditions (for Personal Data) and Schedule 3 Conditions (for Sensitive Personal (Data) – See

☐ Compliance with DPA 8 Prescribed Principles?

☐ Compliance with DPA Schedule 2 Conditions? (Personal Data)

☐ Compliance with DPA Schedule 3 Conditions? (Sensitive Personal Data)

4. By requesting for this information to be disclosed are you relying on the Data Protection Act 2018 Exemption? If so which one?

Section 29

☐ The data is necessary for the prevention or detection of crime

☐ The data is necessary for the apprehension or prosecution of offenders

☐ The data is necessary for the assessment or collection of any tax or duty or of any imposition of a similar nature

Section 35

☐ The data is necessary for the purpose of or in connection with present legal proceedings

☐ The data is necessary for the purpose of or in connection with prospective legal proceedings

☐ The data is otherwise necessary for the purpose of establishing, exercising or defending legal rights

☐ Other exemption *(please name)*

5. Are you disclosing this information under "REASONABLE CAUSE"?

To safeguard a child or adult it is not necessary to complete this form as this information must be disclosed immediately to the relevant authorities. You will though need to have recorded clearly within your own records why you have disclosed this information – please refer to the guidance "Bury Council's Data Sharing a Corporate Guide".

☐ A judgement has been made to share this information because it is within the "public interest" to do so, and it is reasonable, proportionate and necessary.

☐ There is reasonable cause to believe that – give details.

By completing and submitting this form the applicant confirms that the information given on this form is true and that any information provided will be processed in accordance with the Data Protection Principles (apart from any exempt Principle, if applicable, where compliance would be inconsistent with the processing envisaged or there is another reasonable cause). **I am aware of the provisions of Section 170 of the Data Protection Act 2018, regarding the unlawful obtaining of personal data.**

Name of Applicant:	
Title:	
Signed:	
Date:	
All personal data MUST be protected at all times. If sending personal data by e-mail use password protection, encryption or through another secure route	

Please retain a copy of this form for your records and audit purposes.

The decision to release any personal/confidential data must be approved by the head of service unless the head of service has delegated this responsibility to a service manager. In all cases the Head of Service should be aware of the type of personal information being released and how it is released.