Central Bedfordshire Council
www.centralbedfordshire.gov.uk

Information Sharing Policy

May 2018

Security Classification:

OFFICIAL

Approval History

Version No	Approved by	Approval Date	Comments
V1.0	Information Assurance Group (IAG)	18 Aug 15	New Policy
V1.1	Information Assurance Group (IAG)	14 Feb 17	Minor Amendments
V1.2	Information Assurance Group (IAG)	10 Apr 18	GDPR Revisions

Document Author/Owner

Version	Authors	Role
V1.0	Sean Dykes	FOI & Privacy Specialist
V1.1	Sean Dykes	Information Security Manager
V1.2	Sean Dykes	Information Security Manager

Document Governance

Next Review Date	May 19
Publish to Web	Intranet & Internet
Circulation	This policy is to be made available to all CBC staff and observed by all members of staff. This policy should also be published on the Authority's website.
Information Classification	OFFICIAL

Index

1. Introduction

1.1 Information sharing is key to the Authority's goal of delivering better, more efficient services that are coordinated around the needs of the individual. It is essential to enable 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.

1.2 The Authority understands that it is most important that people remain confident that their personal information is kept safe and secure and that staff maintain the privacy of individuals, 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. Factors to consider before sharing information

2.1 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.

2.2 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 is the legal basis for sharing the information?

  The agreement should state on what basis the information is being shared. This will either be consent; contract; legal obligation; protection of vital interests; or public task/official authority. If the information includes special category data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (for id purposes), medical or health details, or details of sex life or sexual orientation) or relates to criminal convictions or activities you can only share if one of the following is **also** applicable: the individual has given explicit consent; it is for the purpose of employment, social security and social protection law; it is to protect vital interests where consent cannot be obtained; legitimate activities by a not-for-profit body with political, philosophical, religious or trade-union aims; the personal data has been made public by the data subject; it is necessary for the establishment, exercise or defence of legal claims; for substantial public interest; for preventative or

occupational medicine, provision of health or social care or the management of such systems; public health; or archiving purposes in the public interest. Where the sharing is being done with consent, you should also ensure that there are adequate procedures in place to deal with the withdrawal of consent.

- What information needs to be shared?

  You should only share the minimum amount of data required to achieve your objective. For example, you might need to share somebody's current name and address but no other information you hold about them such as their date of birth.

- 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 including whether consent to share has been obtained or notice of sharing has been given.

- How can we check the sharing is achieving its objectives?

  You will need to determine a suitable review date and at that time judge whether it is still appropriate and confirm that the safeguards still match the risks (see section 8 below).

- 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 (e.g. statistical information or completely anonymised data).

The flowchart at the end of this guidance should be able to help you further.

3. Sharing of Personal Data

3.1 Since Central Bedfordshire Council deals with sensitive and personal information, it must comply with the General Data Protection Regulation (GDPR) which regulates the processing of such data (as defined in Articles 6 and 9 of the GDPR).

3.2 Processing of personal data must comply with the requirements of all six data protection principles specified within the GDPR unless an exemption applies. The principles are as follows and should be considered when preparing your agreement:

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitations
- Integrity and confidentiality

4. Mythbuster on the General Data Protection Regulation

4.1 The GDPR and other data protection legislation is **not** a barrier to sharing information but provides a framework to ensure that personal information is shared appropriately.

4.2 Data protection law reinforces common sense rules of information handling. It is there to ensure personal information is managed in a sensible way.

4.3 It helps us strike a balance between the many benefits of public organisations sharing information and maintaining and strengthening safeguards and privacy of the individual.

4.4 It also helps us balance the need to preserve a trusted relationship between practitioner and client with the need to share information to benefit and improve the Services provided or, in some instances, protect the public.

5. Information Sharing – Things to Remember

5.1 Remember that the GDPR is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

5.2 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.

5.3 Seek advice from your Manager or the Information Security Manager if you are in any doubt, without disclosing the identity of the person where possible.

5.4 Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. And record this information. You may still share information without consent in the following circumstances:

- **Contract** - the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation** - the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests** - the processing is necessary to protect someone's life.
- **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

5.5 Under GDPR, **legitimate interests** are no longer a legal basis for processing personal data.

5.6 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.

5.7 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 (i.e. follow the GDPR principles).

5.8 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.

6. What Should an Information Sharing Agreement Look Like?

6.1 You will find a guidance document on how to build your information sharing agreement on the information governance pages of the staff intranet. If you are having difficulties, please contact the Information Security Manager or one of the Information Governance team for assistance.

7. Information Sharing Agreement Approval

7.1 Once you have completed your information sharing agreement, it should be forwarded to the Information Security Manager. They will include it in the agenda for

the next available Information Sharing Agreement Authorisation Group (ISAAG) for discussion and approval. The author of the agreement will be required to attend this meeting and they will be notified of the date of inclusion on the agenda. Details of all agreements will be held on a register maintained by the Information Security Manager.

8. Information Sharing Agreement Review

8.1 Information Sharing Agreements should be reviewed annually to check that they are working effectively or can be discontinued if no longer required. This review will be undertaken by the ISAAG who will contact the author for confirmation that it is still in effect as required.

9. Flowchart of Key Questions for Information Sharing