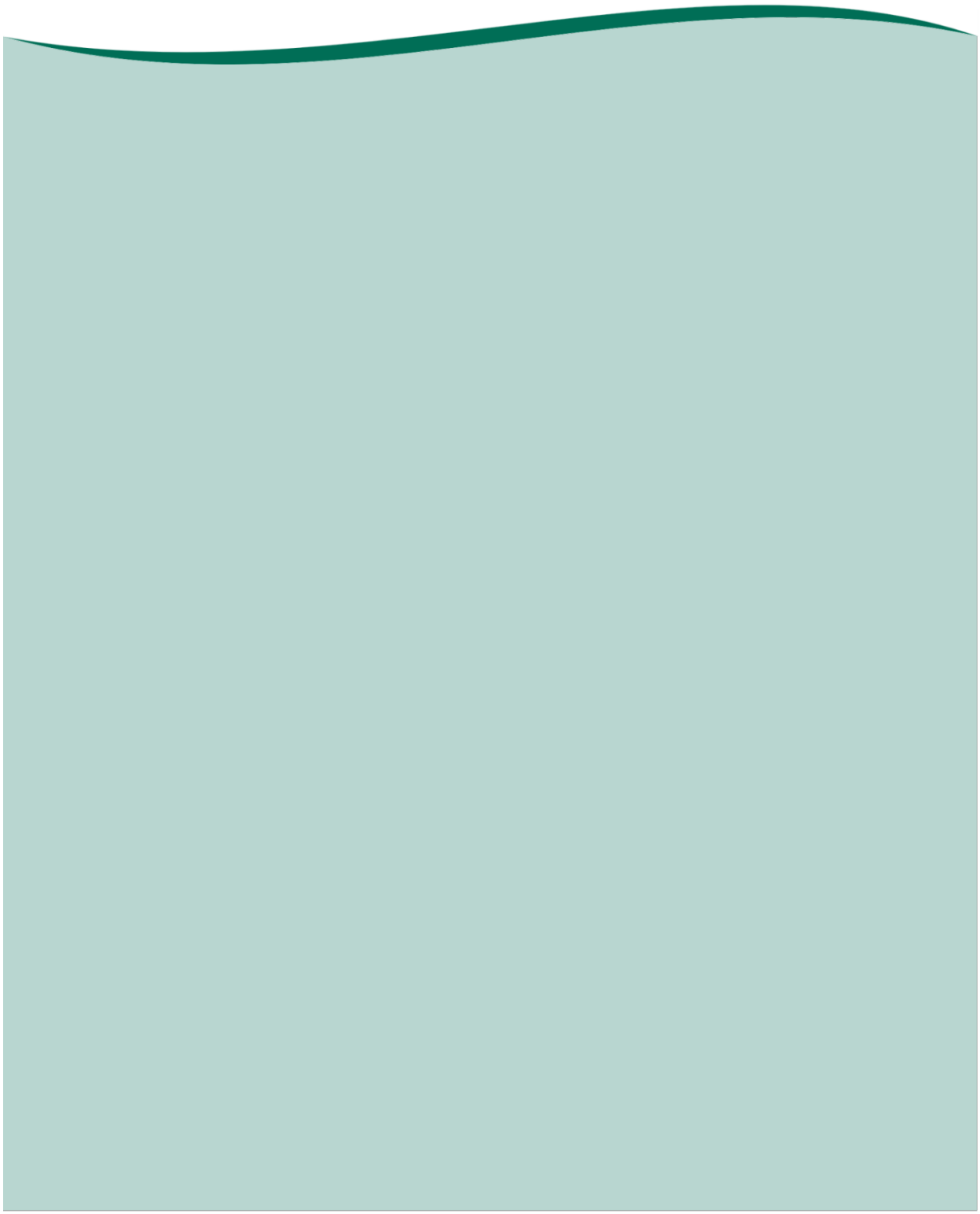
Information Sharing Policy



Document Control

Reference Number:	Version 1.1	Status: Draft	Author(s): Leon Catley, Andrew Holyoake, Tim Way
Amendments:	Updated to reflect GDPR		
Document objectives: To ensure compliance with statutory requirements in relation to the sharing of personal information across Wiltshire Council, internally and externally.			
Intended Recipients: Wiltshire Council Officers			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications: None			
Ratifying Body and Date Ratified	Information Governance Board		
Date of Issue	April 2018		
Review Date	March 2019		
Contact for Review	Information Governance		
SIRO signature			

Associated Documents

Information Governance Policy

Information Governance Management Framework

Information Asset Policy

Privacy Impact Assessment Policy

Data Protection and Subject Access Policy

Information Asset Change Policy

Information Security Policy

Records Management Policy

Legal Framework

Data Protection Act 1998

GDPR Regulation 2016-679 (EU)

Contents

1 Introduction 4
2 Aims of the Policy 4
3 Scope 4
4 Information Sharing 5
5 Personal Data, Special Category Data and Criminal Offence Data 5
6 Types of Information Sharing 6
6.1 Internal sharing 6
6.2 External Sharing: ongoing and regular agreement 6
6.3 External Sharing: one-off case by case basis 6
7 Data Processing on Behalf of the Council 6
8 Data Controller and Data Processor Responsibilities and Obligations 7
9 Privacy Impact Assessments (PIAs) 7
10 Information Sharing Agreements (ISAs) 8
11 Record Keeping 8
12 Information Security 9
13 Staff Communication and Training 9
14 Compliance and Monitoring 9
15 Review 9
16 Appendix A Data Sharing Checklist – systematic data sharing 10
17 Appendix B Data Sharing Checklist - one off requests 11
18 Associated Documentation 12
19 Appendix B Information Sharing Flow Chart 13

1 Introduction

Effective sharing of information across organisational and professional boundaries plays a crucial role in providing efficient services to the public across a range of sectors.

Sharing information about individuals between public authorities is often essential when it is needed to keep people safe or ensure they get the best services. This sharing must only happen when it is legal and necessary to do so and adequate safeguards are in place to protect the security of the information.

Wiltshire Council (the Council) recognises the importance of sharing information and shares personal information with appropriate third parties in order to maximise public service delivery and to meet its statutory responsibilities.

The Council is the data controller for personal information that it processes and will authorise, where appropriate, third parties to process data on its behalf. In these circumstances the third party will be acting as a data processor within the meaning of the relevant legislation.

This policy provides a framework for Council employees and those persons engaged by the Council to confidently and lawfully share personal information. For the purpose of this policy, such persons will be referred to as data users.

2 Aims of the Policy

The aim of this policy is to support and facilitate effective and lawful sharing of information between the Council and third parties within the public, private and third sector.

It promotes the accurate, timely and secure sharing of information in a manner consistent with the Council's legislative responsibilities defined by the EU's General Data Protection Regulation (GDPR) as well as sector led legislation and guidance such as the Caldicott Principles.

3 Scope

This policy applies to all Council employees, elected members contractors, agency workers and any other persons engaged by the Council who need to share personal information as part of their duties.

4 Information Sharing

Information sharing, in the context of this policy, means the disclosure of personal information either between different parts of the same organisation, or from one or more organisations to a third-party organisation or organisations.

This policy covers the sharing of personal information in the following circumstances:

- Internally within the Council
- Externally as an ongoing and regular agreement, or under a data processing contract
- Externally as a one-off case by case basis to another authority or in response to any other lawful request

5 Personal Data, Special Category Data and Criminal Offence Data

In most circumstances, it will be reasonably straight forward to determine whether the information is personal data and therefore regulated by the GDPR.

Personal data means any information from which a living individual is identified or is identifiable.

Special Category Data means personal data that includes the following:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- member of a trade union
- physical or mental health or condition
- genetics
- Biometrics (when used for ID purposes)
- sexual life or orientation

Criminal offence data is no longer treated under GDPR, but covered by the new Data Protection Act 2018.

Criminal offence data requires a lawful basis for processing and for the Council either to have specific legal authority or be processing such data in an official capacity.

- the commission or alleged commission of any offence
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings
- personal data linked to related security measures

The Council may only process such data when the law specifically allows us to or it has an official capacity to do so. Advice is available from the Information Governance Team at dataprotection@wiltshire.gov.uk

6 Types of Information Sharing

6.1 Internal sharing

In order for the Council to provide effective services, it is often necessary for personal information to be shared between different parts of the organisation. In these circumstances the information sharing will need to be justified in accordance with data protection principles and recorded in compliance with this policy.

6.2 External Sharing: ongoing and regular agreement

There is often a need to share personal information externally on a regular basis with appropriate third parties. In these circumstances formal Information Sharing Agreements (ISAs) are required to facilitate the regular and routine sharing of personal information. The Information Asset Change Policy should be referred to where it is identified that an ISA is required.

6.3 External Sharing: one-off case by case basis

There will be times when the Council may need to disclose personal information to a third-party organisation or organisations to either fulfil its statutory obligations or any other lawful request. In these circumstances the information sharing will need to be justified in accordance with data protection principles and recorded in compliance with this policy.

7 Data Processing on Behalf of the Council

When external providers process data on behalf of the Council or processing is hosted on external servers, including those in the cloud, this may only be done under contract. This arrangement is not a data sharing agreement as the ownership of the personal data remains with the Council as data controller. Contracts with service providers must be drawn up with involvement with Procurement Team and Legal Services commercial lawyers and with any additional guidance as required from Information Governance

In such cases, the Council will determine the purposes for which, and the manner in which, any personal data are processed. The requirements of the processing activity will be detailed specifically within the data processing contract. Only processors which satisfy due diligence requirements and provide sufficient guarantees for data security will be authorised by contract to engage in processing data on behalf of the Council.

If a contract to enable data processing is being drawn up, the contract must stipulate;

- That the business relationship is Wiltshire Council is the data controller, and the contractor/service provider is a data processor.
- That the data processor processes the personal data only on the specific documented instructions from the data controller (Wiltshire Council).
- That persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- The processor shall take all measures required in relation to meeting the statutory security requirements.

- The processor shall not engage another sub-processor without prior written authorisation of the data controller.
- The processor will assist the data controller to meet its obligations to exercise data subjects' rights and for ensuring security of personal data, including breach notification within 1 working day of discovery.
- At the choice of the data controller, the processor shall delete or return all the personal data to the controller at the end of the processing service.
- The processor will make available to the controller all information necessary to demonstrate compliance with statutory security requirements and allow and contribute to audits including inspections by or on behalf of the controller.
- Where a processor engages another processor for carrying out specific processing activities, all existing obligations between the controller and the processor shall apply to that other processor. Where there is a failure by that other, the initial processor shall remain liable to the controller for the performance of that other processor's obligations.

8 Data Controller and Data Processor Responsibilities and Obligations

Individual data controllers are responsible for compliance with the relevant legislation and being able to demonstrate that they are compliant with each of the statutory provisions.

Data controllers are also responsible for ensuring (for data for which they are the controller) that the security measures and processing activity performed on it by data processors under their instruction are compliant with the statutory provisions. We do this by making due diligence checks a requirement of the Information Asset Change Process.

GDPR creates new obligations and liabilities for data processors in relation to their accountability, security of data, breach notification, and the need to appoint a data protection officer and keep records of processing activity. The ICO has published guidance on contracts and liabilities between data controllers and processors.

9 Privacy Impact Assessments (PIAs)

PIAs are structured assessments of the potential impact on privacy for new or significantly changed processes. PIAs should form part of the overall risk assessment of the process or project, and are a statutory requirement where the processing of personal data is high risk. See PIA Policy.

10 Information Sharing Agreements (ISAs)

The Council requires Information Asset Owners (IAOs) to record all instances of systematic information sharing within ISAs. These agreements must include the following:

- The purpose or purposes of the sharing and legal basis for sharing
- The type of data to be shared
- The method for sharing securely
- Relevant measures to ensure the accuracy, relevance, and usability (such as the format or type of data) of data shared
- Measures to ensure the security of data shared
- Any relevant arrangements or undertakings in relation to retention of data shared
- Procedures for dealing with
    - subject access requests,
    - queries and complaints and
    - notification to data subjects that their data has been shared
- Review of effectiveness and termination of the sharing agreement
- Instructions to notify originating data controller in the event of any data breach relating to data shared
- Arrangements for regular review of the effectiveness of the agreement

It is the responsibility of the IAO to approve each ISA. Where data is held in a service area governed under Caldicott Principles, each ISA must be signed off by the relevant Caldicott Guardian.

The Information Governance Manager will coordinate a central repository of all Council ISAs. These agreements will be held within the Information Asset Register (IAR).

11 Record Keeping

The Council requires all data users who share personal information to document the decision-making process which justifies the disclosure or non-disclosure of such information. The rationale for decisions should be recorded within the relevant system.

When information is disclosed, data users must record; what information was shared and for what purpose; with whom it was shared; when it was shared; justification for disclosure; and whether it was shared with or without consent.

When requested information is not disclosed, data users should record a description of the request and the reason for declining it.

12 Information Security

Information sharing partners will have different technical, organisational and physical security controls in place. When disclosing personal information data users should ensure that the information is transferred securely. Further guidance can be found here.

13 Staff Communication and Training

This policy will be communicated to staff in line with the Information Governance Communication and Engagement Strategy.

Training related to this policy will be delivered in line with the Information Governance Training Strategy 2017-2019.

14 Compliance and Monitoring

Compliance with this policy will be monitored and reviewed by the Information Governance Board.

15 Review

This policy will be reviewed at least annually or when required by changed circumstances.

16 Appendix A Data Sharing Checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have a lawful basis to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

17 Appendix B Data Sharing Checklist - one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have a legal basis to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
- Only share what is necessary.
- Distinguish fact from opinion.
- How should the information be shared?
- Information must be shared securely.
- Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

- If you share information you should record:
- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

18 Associated Documentation

- Seven Golden Rules for Information Sharing (Advice for practitioners providing safeguarding services to children, young people, parents and carers)
- ICO Data Sharing Code of Practice
- ICO Data Sharing Checklists
- Caldicott Principles

19 Appendix B Information Sharing Flow Chart