

Information Sharing Policy

1. Aim

The aim of this policy is to support and facilitate effective and lawful sharing of information between Armthorpe Parish 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 Armthorpe Parish Council's legislative responsibilities defined by the Data Protection Act 1998 as well as sector led legislation and guidance.

2. 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.

As Armthorpe Parish Council shares large amounts of data with defined third parties in order to maximise public service delivery, and to meet its statutory responsibilities, it is important to maintain trust in the way that this is achieved by demonstrating that it is done so in a lawful, responsible and secure manner.

3. Types of information sharing

Information sharing in the context of this policy means the sharing of personal data from one or more organisations to another. The two main types of information sharing are:

- Systematic, routine, data sharing where the same data sets are shared between the same organisations for an established and agreed purpose; and
- Exceptional, one off decisions, to share data for any of a range of appropriate and agreed purposes.

4. Personal data and sensitive personal data

In most circumstances it will be reasonably straightforward to determine whether the information is personal data and therefore regulated by the Data Protection act.

If a living individual can be identified from the data, or, from the data and other information in Armthorpe Parish Council's possession, or likely to come into Armthorpe Parish Council's possession and it relates to an identifiable living individual, whether in personal or family life, business or profession, it is personal data.

Sensitive personal data means personal data consisting of:

- The racial or ethnic origin of the data subject,
- His/her political opinions;
- His/her religious beliefs or other beliefs of a similar nature;

- Whether he/she is a member of a trade union;
- His/her physical or mental health or condition;
- His/her sexual life;
- The commission or alleged commission by him/her of any offence, or;
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

5. Data Protection Act 1998

The Data Protection Act 1998 applies to personal data and gives individuals a number of important rights to ensure that personal information covered by the act is processed lawfully.

It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing.

Key principles in the Data Protection Act 1998 state that personal information must:

- Be processed fairly and lawfully;
- Be obtained for a specified and lawful purpose and not processed in a manner incompatible with that purpose;
- Be adequate, relevant and not excessive for the purpose;
- Be accurate and, where necessary kept up to date;
- Not kept longer as is necessary;
- Be processed in accordance with the rights of the data subject;
- Be subject to appropriate technical and organisational measures designed to prevent unauthorised/unlawful processing and accidental loss, destruction or damage;
- Not to be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6. Before you decide to share personal data

Before sharing personal data you must identify the objective of sharing and carefully consider the following factors:

- What is the sharing meant to achieve?
- Could the objective be achieved without sharing the data or by anonymising it?
- What is the legal basis for sharing the information?
- What information needs to be shared and who requires access?
- When and how should it be shared?
- How can we check the sharing is achieving its objectives?
- What risk does the data sharing pose?
- How will any shared data be kept up to date?

7. Lawful sharing

You must ensure personal data is only shared where it is fair and lawful. The first principle of the Data Protection Act 1998 requires that you must satisfy one or more conditions in order to legitimise the processing i.e. sharing of personal data.

Sharing involving sensitive personal data can be undertaken only when a further more exacting condition

has been satisfied in accordance with the first data protection principle.

Conditions for sharing are set out at Annex A to this policy.

8. Fairness and transparency

You must ensure that personal data is shared fairly and in a way that is reasonable. People should generally be aware who you are sharing their personal data with and what it is being used for.

Armthorpe Parish Council will maintain a privacy notice in line with the Information Commissioners Office Code of Practice. The privacy notice is available on the Armthorpe Parish Council website.

To support a transparent approach you should consider proactively communicating a privacy notice, for example when sharing sensitive personal data or where sharing the data will have a significant effect on the individual.

You must work together with partner organisations to ensure that the individuals concerned know who has, or will have, their data and what it is being used for.

9. Individual Rights

The Data Protection Act gives individuals certain rights over their personal data. These include:

- The right to access personal data held about them;
- The right to know how their data is being used; and
- The right to object to the way their data is being used.

An information sharing initiative must take into consideration individual rights and have in place mechanisms to support individuals.

If a significant number of objections, negative comments or other expressions of concern are received regarding a particular information sharing process, a review of the data sharing in question will be carried out.

10. Security of information

Information sharing partners will have varying degrees of technical, physical and procedural security controls in place.

It is important therefore to ensure consistency in approach by agreeing common minimum standards which can be achieved by all partners and which provides appropriate assurance when sharing personal data.

11. Privacy Impact Assessment

Privacy Impact Assessments are intended as a means for Armthorpe Parish Council to identify and minimise the privacy risks concerned with sharing information and support our requirement to comply with data protection law.

12. Information Sharing Agreements

You must document instances of systematic information sharing within information within information

sharing agreements. The Information Sharing Agreements must include:

- The purpose, or purposes, of the sharing;
- The potential recipients or types of recipient and the circumstances in which they will have access;
- The data to be shared;
- The process for sharing;
- Data quality – accuracy, relevance, usability etc;
- 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; and
- Sanctions for failure to comply with the agreement or breaches by individual staff.

It is the responsibility of the Information Asset Owner to approve information sharing agreements.

Information Service Agreements must be reviewed regularly to ensure that they continue to meet the needs set out. This must be done on an annual basis.

13. Ad hoc or 'one off' sharing

It may not always be possible to document the sharing of information in an emergency or time dependent situation and sharing may depend primarily on the exercise of professional judgement.

Where this is the case you must make a record as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place.

In the event that ad hoc instances of information sharing become a regular occurrence, it must be considered whether it is necessary to amend an existing information sharing agreement to reflect this change or whether a separate information sharing agreement is required.

14. Information Requests and Disclosures

Armthorpe Parish Council will respond to all information requests and disclosures in accordance with the Data Protection Act 1998, the Freedom of Information Act 2000, and relevant local government transparency requirements.

Requests for personal data made by individuals (Subject Access Requests) will be managed in line with the Council's Data Protection Policy and associated procedures to ensure lawful and timely responses.

Disclosures of personal data to third parties will only be made where one or more of the lawful conditions in Annex A are satisfied. Each disclosure must be assessed to confirm that it is:

- Fair, lawful, and proportionate;
- Necessary for the stated purpose; and
- Accompanied by appropriate safeguards to protect the rights and freedoms of the data subject.

Where information is requested by law enforcement, regulators, or other statutory bodies, disclosure will be undertaken only where there is a clear legal power or obligation to do so, and the disclosure is appropriately recorded.

All decisions to disclose personal data must be documented, including the purpose of disclosure, the recipient, the lawful basis relied upon, and any conditions or restrictions applied.

Where a disclosure is refused, the reason for refusal and any advice given to the requester must also be recorded.

Council staff involved in handling information requests or disclosures must complete periodic data protection and information governance training to ensure continuing compliance with legislation and Council policy.

Dated: 6th October 2025

Approved: 2nd December 2025

To be Reviewed: Annually

Annex A: Conditions for the Fair and Lawful Sharing of Personal Data

A.1 General Principles

Under the first principle of the Data Protection Act 1998, personal data must be processed and shared fairly and lawfully. Personal data may only be shared where one or more of the conditions set out in Schedule 2 of the Act are satisfied. Where the sharing involves sensitive personal data, one or more of the additional and more exacting conditions in Schedule 3 must also be met.

A.2 Conditions for Processing and Sharing Personal Data (Schedule 2)

1. Consent – The data subject has given their consent to the sharing or processing of their personal data.
2. Contractual necessity – The sharing is necessary for the performance of a contract with the data subject, or to take steps at their request prior to entering into a contract.
3. Legal obligation – The sharing is necessary for compliance with a legal obligation to which the Council is subject (other than an obligation imposed by contract).
4. Vital interests – The sharing is necessary to protect the vital interests of the data subject, such as life or serious health and safety concerns.
5. Public functions – The sharing is necessary for the performance of a function carried out in the public interest or in the exercise of official authority.
6. Legitimate interests – The sharing is necessary for the legitimate interests of the Council or a third party, except where such interests are overridden by the rights and freedoms of the data subject.

A.3 Additional Conditions for Processing and Sharing Sensitive Personal Data (Schedule 3)

In addition to one of the Schedule 2 conditions, at least one of the following Schedule 3 conditions must also be satisfied where sensitive personal data is shared:

7. Explicit consent – The data subject has given explicit consent to the sharing or processing.
8. Employment law obligations – The sharing is necessary for carrying out obligations or exercising specific rights under employment law.
9. Vital interests – The sharing is necessary to protect the vital interests of the data subject or another person where consent cannot be obtained or is unreasonable to seek.
10. Non-profit organisations – The sharing is carried out by a not-for-profit body (such as a charity or council) in the course of its legitimate activities and relates only to members, former members or persons in regular contact with it.
11. Information made public by the data subject – The data has been deliberately made public by the individual concerned.
12. Legal proceedings – The sharing is necessary for establishing, exercising or defending legal rights or in connection with legal proceedings.
13. Public administration and justice – The sharing is necessary for the administration of justice or the exercise of statutory, governmental, or other public functions.
14. Medical purposes – The sharing is necessary for medical purposes and carried out by a health professional or another person under a duty of confidentiality.
15. Substantial public interest – The sharing is necessary for reasons of substantial public interest, as set out in law.

A.4 Accountability and Record Keeping

- The lawful basis for sharing personal data must be clearly identified and documented.
- Where consent is relied upon, it must be explicit, informed, and evidenced in writing.
- Where sensitive personal data is shared, additional security and confidentiality safeguards must be applied.
- All information sharing decisions must be recorded, including the rationale, legal basis, and any conditions or restrictions attached to the sharing.