



Burston and Shimpling Parish Council

Community Resilience Plan - GDPR Data Protection Policy

1. Policy Statement

This policy sets out how Burston and Shimpling Parish Council handles personal data for the purpose of the Community Resilience Plan, in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Purpose of Processing

- 2.1. Identify vulnerable residents needing assistance during emergencies (e.g., flooding, power outages).
- 2.2. Coordinate volunteer responses.
- 2.3. Maintain a list of local resources and contacts.
- 2.4. Communicate emergency information.

3. Data We Collect (Including Special Category Data)

We may collect:

- 3.1. **General:** Name, address, telephone number, email address.
- 3.2. **Special Category Data:** Specific needs, disabilities, or medical conditions that make a resident vulnerable in an emergency.

4. Lawful Basis for Processing

We process this data based on:

- 4.1. **Public Task:** To perform tasks in the public interest for community safety.
- 4.2. **Vital Interests:** To protect someone's life in an emergency situation.
- 4.3. **Consent:** Explicit consent will be sought from residents before adding them to a vulnerable person list.

5. Data Retention

Data collected for the resilience plan will be kept for no longer than necessary.

5.1. Vulnerable resident lists will be reviewed annually.

5.2. Consent will be re-confirmed, and data deleted if no longer needed or if consent is withdrawn.

6. Data Security and Sharing

6.1. Data is securely stored by the Clerk and Resilience Plan Co-ordinator and only shared with approved volunteers/emergency services on a "need to know" basis during an incident.

6.2. Hard copies are kept in locked cabinets; digital copies are password-protected.

6.3. Volunteers handling this data must abide by this policy

7. Individual Rights

Residents have the right to:

7.1. Access the data held about them.

7.2. Request correction of inaccurate data.

7.3. Request erasure of their data (the right to be forgotten).

7.4. Withdraw consent at any time.

8. Data Breach Procedure

If a breach occurs, it will be reported to the Information Commissioner's Office (ICO) within 72 hours if it poses a risk to the rights and freedoms of individuals.