# Great Tey Parish Council

## Data Breach Policy

### 1. Purpose:

Great Tey Parish Council holds personal and confidential information as part of its work. This policy sets out how the Council will respond to a data breach in a timely, effective, and compliant manner.

A data breach can cause harm to individuals and expose the Council to legal and reputational risks. Having a clear response plan helps ensure swift action, reduces stress, and supports recovery should an incident occur.

This policy applies to all councillors, employees, contractors, and volunteers.

### 2. Definition of a Data Breach:

A data breach is any incident that results in the accidental or unlawful:

- Loss of data
- Destruction of data
- Alteration of data
- Unauthorised disclosure of data
- Unauthorised access to data

Examples include (but are not limited to):

- A lost or stolen laptop, phone, or USB device containing council data
- An email containing personal data sent to the wrong recipient
- Hacking, malware, or ransomware attacks
- Paper files being lost or accessed without authorisation

### 3. Responsibility:

Overall responsibility for managing and responding to data breaches rests with the Clerk, who leads the investigation and response on behalf of the Council.

All councillors and staff are responsible for:

- Remaining alert to potential data breaches
- Acting promptly if a breach is suspected
- Cooperating fully with any investigation

### 4. Reporting a Data Breach:

Any suspected or actual data breach must be reported immediately to the Clerk, regardless of how minor it may appear.

Reports should include:

- What happened

- When it happened
- What data may be affected
- Who may be affected
- Any action already taken

Delays in reporting may increase risks to individuals and may prevent the Council from meeting legal obligations.

### 5. Timescales and Immediate Actions:

Upon being notified of a potential data breach, the Clerk will:

1. Within 24 hours:
    - Assess the nature and seriousness of the breach
    - Take immediate steps to contain the breach and prevent further damage
2. Within 72 hours:
    - Determine whether the breach must be reported to the Information Commissioner's Office (ICO)
    - Prepare and submit a report to the ICO where required
    - Consider whether affected individuals need to be informed

The 72-hour timeframe begins from the point at which the Council becomes aware of the breach.

### 6. Escalation and Authority:

- Only the Clerk (or a formally authorised deputy) is permitted to liaise with external bodies, including the ICO, insurers, IT providers, or legal advisers.
- Councillors and staff must not attempt to resolve serious breaches independently or contact affected individuals without authorisation.
- Significant breaches may be escalated to the Chair of the Council as appropriate.

### 7. Record Keeping:

All data breaches, including near misses and minor incidents, will be documented in a breach log maintained by the Clerk.

Records will include:

- Details of the incident
- Actions taken to contain and resolve it
- Decisions regarding notification
- Lessons learned and any changes made to prevent recurrence

This record supports accountability, learning, and continuous improvement.

8. Review:

This policy will be reviewed regularly and updated as required to reflect changes in legislation, guidance, or council procedures.

1. Purpose:

Great Tey Parish Council holds personal and confidential information as part of its work. This policy sets out how the Council will respond to a data breach in a timely, effective, and compliant manner.

A data breach can cause harm to individuals and expose the Council to legal and reputational risks. Having a clear response plan helps ensure swift action, reduces stress, and supports recovery should an incident occur.

This policy applies to all councillors, employees, contractors, and volunteers.

2. Definition of a Data Breach:

A data breach is any incident that results in the accidental or unlawful:

- Loss of data
- Destruction of data
- Alteration of data
- Unauthorised disclosure of data
- Unauthorised access to data

Examples include (but are not limited to):

- A lost or stolen laptop, phone, or USB device containing council data
- An email containing personal data sent to the wrong recipient
- Hacking, malware, or ransomware attacks
- Paper files being lost or accessed without authorisation

3. Responsibility:

Overall responsibility for managing and responding to data breaches rests with the Clerk, who leads the investigation and response on behalf of the Council.

All councillors and staff are responsible for:

- Remaining alert to potential data breaches
- Acting promptly if a breach is suspected
- Cooperating fully with any investigation

4. Reporting a Data Breach:

Any suspected or actual data breach must be reported immediately to the Clerk, regardless of how minor it may appear.

Reports should include:

- What happened
- When it happened
- What data may be affected
- Who may be affected
- Any action already taken

Delays in reporting may increase risks to individuals and may prevent the Council from meeting legal obligations.

### 5. Timescales and Immediate Actions:

Upon being notified of a potential data breach, the Clerk will:

3. Within 24 hours:
    - Assess the nature and seriousness of the breach
    - Take immediate steps to contain the breach and prevent further damage
4. Within 72 hours:
    - Determine whether the breach must be reported to the Information Commissioner's Office (ICO)
    - Prepare and submit a report to the ICO where required
    - Consider whether affected individuals need to be informed

The 72-hour timeframe begins from the point at which the Council becomes aware of the breach.

### 6. Escalation and Authority:

- Only the Clerk (or a formally authorised deputy) is permitted to liaise with external bodies, including the ICO, insurers, IT providers, or legal advisers.
- Councillors and staff must not attempt to resolve serious breaches independently or contact affected individuals without authorisation.
- Significant breaches may be escalated to the Chair of the Council as appropriate.

### 7. Record Keeping:

All data breaches, including near misses and minor incidents, will be documented in a breach log maintained by the Clerk.

Records will include:

- Details of the incident
- Actions taken to contain and resolve it
- Decisions regarding notification
- Lessons learned and any changes made to prevent recurrence

This record supports accountability, learning, and continuous improvement.

### 8. Review:

This policy will be reviewed regularly and updated as required to reflect changes in legislation, guidance, or council procedures.