DATA PROTECTION POLICY

Document Review History:

Document Ref: POL/DP

Status: Approved

Version: 2.3

Date of Approval: 07 October 2026

Date of Next Review: October 2028

Version Control:

Version: 2.3
Amended by: Clerk
Details of amendment(s): Bi-annual review. No update to LALC model template, still version revised March 2018 (GDPR). No updates.

The Data Protection Policy

Saxilby with Ingleby Parish Council ('the council') recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

The GRPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled, and used. The GDPR applies to anyone holding personal information about people, whether held electronically or on paper. The council has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, officers and councillors must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**
  This means that personal information should only be collected from individuals if officers have been open and honest about why they want the personal information.

- **Data is processed for specified purposes only**
  This means that data is collected for specific, explicit, and legitimate purposes only.

- **Data is relevant to what it is needed for**
  Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**
  Personal data should be accurate, if it is not, it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**
  Individuals must be informed, upon request, of all the personal information held about them.

- **Data is kept securely**
  There should be protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Storing and accessing data

The council recognises its responsibility to be open with people when taking personal details from them. This means that officers must be honest about why they want a particular piece of personal information.

The council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the parish council office and are not available for public access. All data stored on council computers[1] are password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of the council's document retention policy, it will be shredded or securely deleted from the computer.

The council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, via email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period the Council intend to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, the council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the subject.

Individuals have the right to:

- Have their data rectified if it is incorrect
- Request erasure of the data
- Request restriction of processing of the data
- Object to data processing

Specific rules do apply to these requests.

Confidentiality

Councillors and officers must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Linked policies: Document Retention & Disposal Policy; Information Security / IT & Cyber Security Policy; Confidentiality Policy; Councillor Code of Conduct; Subject Access Request (SAR) Procedure; Complaints Policy; Freedom of Information (FOI) Policy & Publication Scheme; Data Breach Procedure; Staff Handbook (Data Handling Section); Councillor Induction & Training Policy.

[1] Including the server and any devices used to access this