



STITHIANS PARISH COUNCIL

DATA PROTECTION AND GDPR POLICY

Adopted:

Review Date:

Policy Owner: Parish Clerk

Approved by: Stithians Parish Council

1. Purpose

Stithians Parish Council is committed to protecting the privacy and personal information of residents, councillors, staff, volunteers, contractors, suppliers and other individuals with whom the Council has contact.

This policy sets out how the Council will collect, use, store, share, retain and securely dispose of personal information in accordance with applicable data protection legislation.

The Council will comply with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, the **Privacy and Electronic Communications Regulations (PECR)** and other relevant information rights legislation, as amended from time to time. The Council will also have regard to current guidance issued by the **Information Commissioner's Office (ICO)**.

2. Scope

This policy applies to:

- the Parish Council as a corporate body;
- the Parish Clerk and other employees;
- all Parish Councillors;
- volunteers and persons acting on behalf of the Council;
- contractors and suppliers where they process personal information for the Council.

It applies to personal information held in any form, including:

- paper records;
- emails;
- electronic documents;
- databases and spreadsheets;
- photographs and images;
- telephone records;
- website enquiries;
- social media;
- correspondence;
- financial and payment records;
- recordings where applicable.

Personal information must be treated in accordance with this policy whether it is held on Council equipment, a Council-managed system or, where authorised, a councillor's or employee's device

3. The Council's Responsibility

Stithians Parish Council is the **Data Controller** for personal information that it determines the purpose and manner of processing. The Council has overall responsibility for ensuring that personal information is handled lawfully and securely.

The Council will maintain appropriate documentation to demonstrate compliance with data protection legislation, including:

- this Data Protection Policy;
- Privacy Notices;
- a Record of Processing Activities/Data Register;
- a Data Retention Schedule;
- records of data breaches;
- Data Protection Impact Assessments where required.

The Council will review its arrangements regularly and make improvements where necessary. The ICO identifies accountability as a fundamental data protection requirement: the Council must not only comply with the law but be able to demonstrate that it has done so.

4. Data Protection Lead

The Council will appoint a **Data Protection Lead**, normally the Parish Clerk, to manage the Council's day-to-day data protection arrangements. The Data Protection Lead will:

- act as the first point of contact for data protection matters;
- maintain the Council's data protection documentation;
- deal with requests from individuals concerning their personal information;
- maintain the data breach register;
- ensure appropriate privacy notices are in place;
- advise councillors and staff on data protection requirements;
- arrange appropriate training and awareness;
- review data protection arrangements regularly;
- seek specialist advice from the ICO, Cornwall Association of Local Councils, NALC or an appropriately qualified adviser where necessary.

The Council may appoint an external Data Protection Officer or specialist adviser if it considers this appropriate.

5. What is Personal Data?

Personal data is information relating to an identified or identifiable living individual. Examples relevant to Parish Council activities include:

- names and addresses;
- telephone numbers;
- email addresses;
- signatures;
- correspondence from residents;
- complaints and enquiries;
- photographs identifying individuals;
- information about councillors, staff or volunteers;
- payment and bank details;
- payroll information;
- information relating to allotments, burials, bookings or other Council services;
- information contained in planning or other correspondence where individuals can be identified.

Some information requires additional protection, including health information and other **special category data**. The Council will only collect and use such information where there is a lawful basis and, where required, an additional condition for processing.

6. Data Protection Principles

The Council will comply with the data protection principles.

Personal data must be:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and kept up to date where necessary.
5. Kept only for as long as necessary.
6. Processed securely, protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Council will also demonstrate accountability for its compliance.

7. Lawful Basis for Processing

Before collecting or using personal data, the Council will identify an appropriate lawful basis. Depending on the circumstances, this may include:

- **Legal obligation** – where the Council is required by law to process the information;
- **Public task** – where processing is necessary for the Council to perform its functions;
- **Contract** – where processing is necessary to enter into or perform a contract;
- **Legitimate interests** – where applicable and where the Council's interests are not overridden by the individual's rights;
- **Consent** – where appropriate and where an individual has a genuine choice.

Consent will not normally be used where the Council has another more appropriate lawful basis. The lawful basis for significant or recurring processing activities will be recorded in the Council's data register.

8. Parish Council Meetings, Agendas and Minutes

The Council operates in an open and transparent manner and is subject to statutory requirements concerning public meetings, agendas and minutes. Personal information will not automatically be removed simply because it is personal data.

However, the Council will consider data protection requirements when preparing agendas, reports and minutes and will only publish personal information where there is a lawful basis for doing so. Where appropriate, unnecessary personal information will be removed or redacted before documents are published.

Care will be taken when handling:

- complaints;
- allegations concerning individuals;
- personal circumstances;
- children's information;
- health information;
- financial information;
- information relating to vulnerable individuals.

Councillors and members of the public should not include unnecessary personal information in correspondence intended for publication.

9. Councillors and Personal Information

Councillors frequently receive personal information in connection with their role.

Councillors must:

- only collect information necessary for legitimate Council business;
- keep personal information secure;
- not use Council information for private purposes;
- not disclose personal information to other people unless authorised and lawful;
- not forward confidential correspondence unnecessarily;
- use appropriate passwords and security;
- avoid storing Council information permanently on personal devices where a Council system is available;
- report any suspected loss or disclosure of personal information to the Clerk immediately.

Councillors must not assume that information received in their capacity as a councillor is their personal information to retain or use as they wish.

Where a councillor receives a request or correspondence containing personal information which relates to Council business, it should normally be forwarded to the Clerk for appropriate recording and handling.

10. Email and Electronic Communications

Council business should normally be conducted using the Council's authorised email arrangements. Personal information should not be sent by email unless there is a legitimate reason to do so. Where personal information is sent electronically, appropriate precautions must be taken, including:

- checking the recipient before sending;
- using appropriate password protection or encryption where necessary;
- avoiding unnecessary personal information in the subject line;
- using BCC rather than CC when sending emails to multiple individuals whose addresses should not be disclosed;
- not forwarding confidential information unnecessarily.

11. Telephone, Messaging and Social Media

Information received by telephone, text message, WhatsApp or social media may constitute Council records where it relates to Council business.

Personal information must not be transferred or shared through messaging services unless there is a legitimate Council purpose and appropriate security is available.

Where Council business is conducted through a personal device or messaging service, relevant information should be transferred to the Council's official records where necessary and should not be retained indefinitely on the personal device.

Councillors must not use social media to disclose confidential or personal information obtained through their Council role.

12. Photographs and Images

The Council may take and publish photographs in connection with Council activities, events and publicity.

Before publishing identifiable photographs, the Council will consider:

- the purpose for which the photograph is being used;
- whether individuals have a reasonable expectation of privacy;
- whether consent is appropriate;
- whether children are involved;
- whether publication is necessary and proportionate.

Photographs will not be retained indefinitely where there is no continuing Council purpose.

13. Children and Vulnerable Individuals

The Council will take additional care when processing information relating to children or vulnerable individuals. Only information necessary for the particular Council activity will be collected.

Where consent is required, the Council will ensure that appropriate consent arrangements are used.

Personal information relating to children or vulnerable individuals will not be published or shared unnecessarily.

14. Data Sharing

The Council will only share personal information where there is a lawful basis for doing so. Information may, where appropriate, be shared with organisations such as:

- Cornwall Council;
- Police;
- South West Water;
- Utility Providers;
- Auditors;
- Contractors;
- Payroll providers;
- Insurers;
- other public bodies.

Before sharing information, the Council will consider:

1. Why is the information being shared?
2. Is there a lawful basis?
3. Is the information necessary and proportionate?
4. Is the recipient entitled to receive it?
5. Is the information being transferred securely?

Where another organisation processes personal data on behalf of the Council, an appropriate written agreement will be put in place where required.

15. Contractors and Data Processors

The Council may use external organisations to process personal data, including providers of:

- Payroll Services;

- Accounting Systems;
- Website Services;
- Email Systems;
- Cloud Storage;
- CCTV or security services;
- Event or Booking systems.

The Council will take reasonable steps to ensure that processors provide sufficient guarantees regarding the security and lawful processing of personal data. Contracts with processors will include appropriate data protection provisions where required.

16. Data Security

The Council will take appropriate technical and organisational measures to protect personal information. This will include, as appropriate:

- strong passwords;
- password protection on devices;
- appropriate antivirus and security software;
- software updates;
- secure backups;
- restricted access to confidential information;
- secure disposal of paper records;
- secure disposal or wiping of electronic devices;
- appropriate physical security for paper files and equipment.

Access to personal information will be limited to those who need it for legitimate Council business.

17. Personal Devices

Where councillors or staff use personal devices for Council business, they remain responsible for protecting Council information held on those devices. Council information should not be stored unnecessarily on personal devices.

Where possible:

- devices should be password or biometric protected;
- operating systems and software should be kept up to date;
- Council information should be transferred to the Council's official records;
- unnecessary copies should be deleted;
- lost or stolen devices containing Council information must be reported immediately.

18. Data Breaches

A data breach may include:

- sending personal information to the wrong person;
- losing paperwork;
- losing a laptop, tablet or phone;
- unauthorised access to files;
- accidental publication of personal information;
- disclosure of information without authority;
- malware or hacking;
- unauthorised use of Council information.

Any suspected or actual data breach must be reported to the Clerk/Data Protection Lead **immediately**. The Clerk will:

1. Contain the breach where possible.
2. Establish what information has been affected.
3. Assess the risk to individuals.
4. Record the incident.
5. Decide whether notification to the ICO is required.
6. Notify affected individuals where required.
7. Take steps to prevent a recurrence.

Where a breach is reportable, the Council will comply with the applicable statutory timescale.

19. Individual Rights

Individuals have rights concerning their personal information, subject to the circumstances and exemptions provided by law. These may include rights to:

- be informed about the use of their information;
- access their personal information;
- have inaccurate information corrected;
- request deletion in certain circumstances;
- restrict processing in certain circumstances;
- object to certain processing;
- request information about automated decision-making where applicable.

All requests concerning an individual's personal information should be referred to the Clerk/Data Protection Lead promptly.

The Council will not ignore a request simply because it has not been described as a formal "Subject Access Request".

20. Subject Access Requests

A person may ask the Council what personal information it holds about them. The Clerk will:

- identify the request;
- verify the identity of the requester where necessary;
- identify relevant records;
- consider whether any information is exempt from disclosure;
- provide the appropriate response within the statutory timeframe.

Requests will be recorded and monitored to ensure that statutory deadlines are met.

21. Freedom of Information and Environmental Information

Data protection does not prevent the Council from complying with its obligations under:

- the Freedom of Information Act 2000; and
- the Environmental Information Regulations 2004.

Where a request involves personal information, the Council will consider both the relevant access legislation and data protection legislation. The Council will not automatically disclose personal information simply because it has been requested under FOI or EIR.

Where necessary, personal information will be redacted or withheld in accordance with the relevant legislation.

The Council's separate FOI/EIR Policy and Procedure should be read alongside this policy.

22. Data Retention and Disposal

The Council will not retain personal information indefinitely. Information will be retained only for as long as there is a legitimate legal, administrative or operational reason to do so.

The Council will maintain a Data Retention Schedule identifying appropriate retention periods for different categories of information.

When information is no longer required, it will be securely disposed of. Paper records containing personal information will be securely shredded or otherwise securely destroyed. Electronic records will be securely deleted where appropriate.

Retention requirements relating to statutory records, financial records, employment records, burial records and other Council records will be taken into account.

23. Electronic Communications – Emails and Messages

Emails and other electronic communications relating to Parish Council business are Council records where they contain information required to demonstrate, evidence or support the Council's activities, decisions or actions.

The Council will not retain emails or other electronic messages indefinitely simply because they are held electronically. Communications will be retained in accordance with the Council's Retention Schedule and deleted when they are no longer required, subject to any statutory, legal, audit, historical or other legitimate requirement for continued retention.

Where an email or electronic message forms part of an official Council record, the relevant information should be transferred to the appropriate Council record or filing system and retained in accordance with the applicable retention period.

Routine, duplicate or transitory communications should be deleted when they are no longer required.

Councillors and officers must take reasonable care when using email, text messaging, WhatsApp or other electronic communication for Council business. Personal data must be handled securely and communications relating to Council business must be retained or deleted in accordance with this Policy and the Council's Retention Schedule.

The Council will periodically review electronic communications and delete personal data and other information that is no longer required.

24. Privacy Notices

The Council will maintain appropriate Privacy Notices explaining:

- what personal information is collected;
- why it is collected;
- the lawful basis for processing;
- who information may be shared with;

- how long information is retained;
- individual rights;
- how to contact the Council about data protection;
- how to complain to the ICO.

Privacy Notices will be reviewed when the Council introduces significant new processing activities.

25. Data Protection by Design

Data protection will be considered before introducing new systems, services or activities involving personal information. The Council will ask:

- What personal information will be collected?
- Why is it needed?
- Who will have access?
- Where will it be stored?
- How long will it be kept?
- Who will it be shared with?
- What could go wrong?
- What security measures are required?

A **Data Protection Impact Assessment (DPIA)** will be undertaken where required by law or where a proposed activity is likely to create a high risk to individuals.

The ICO recommends considering data protection at the beginning of projects rather than attempting to address privacy issues after a system or activity has been introduced.

26. Training and Awareness

The Council will ensure that councillors and staff understand their responsibilities concerning personal information.

Councillors and staff are expected to raise concerns where they are unsure how personal information should be handled.

27. Data Protection Fees and ICO Registration

The Council will maintain its registration with the Information Commissioner's Office where required and will pay any applicable data protection fee.

The Clerk will monitor the Council's registration and renewal requirements.

The ICO confirms that organisations processing personal information generally need to pay the statutory data protection fee unless an exemption applies.

28. Records and Accountability

The Council will maintain sufficient records to demonstrate compliance with data protection legislation.

These will include, where applicable:

- Data Register/Record of Processing Activities;
- Privacy Notices;
- Data Retention Schedule;
- Data Breach Register;
- Data Protection Impact Assessments;

- Processor agreements;
- relevant consent records;
- records of data protection requests;
- evidence of training and reviews.

The Council will review these records periodically.

29. Complaints

Any individual who has concerns about how the Council has handled their personal information should contact the Parish Clerk in the first instance.

The Council will investigate complaints fairly and promptly.

Individuals also have the right to complain directly to the Information Commissioner's Office.

30. Review of Policy

This policy will be reviewed at least annually and sooner if:

- there is a significant change in data protection legislation;
- ICO guidance changes;
- the Council introduces significant new systems or activities;
- a serious data breach occurs;
- an audit identifies a need for change.

The Council will ensure that associated documents, including its Privacy Notice, Retention Schedule and Data Register, remain consistent with this policy.

31. Related Documents

This policy should be read alongside the Council's:

- Privacy Notice;
- Data Retention Schedule;
- Freedom of Information Policy and Procedure;
- Environmental Information Regulations Procedure;
- Document Retention Policy;
- Information Security arrangements;
- Email and IT arrangements;
- Complaints Procedure;
- Councillor Code of Conduct;
- Social Media Policy;
- Employee/Staff policies where applicable.