FOXTON PARISH COUNCIL DATA PROTECTION POLICY

1. Introduction

This privacy policy is provided to you by Foxton Parish Council (the Parish Council) which is the data controller for your data.

We hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.

This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2. Scope

This policy applies to all councillors and staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3. Data Protection Officer

The Parish Council has appointed CAPALC as an external Data Protection Officer to ensure compliance with Data Protection legislation. Their contact details are:

CAPALC, PO Box 181, St Ives, PE27 9DR

Tel: 01480 375 629 Email: accounts@capalc.org.uk

4. Data Protection Terminology

Business purposes - The purposes for which personal data may be used by us such as personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.

Council purposes include the following:

- *Compliance with our legal, regulatory and corporate governance obligations and good practice*

- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*
- *Ensuring Council policies are adhered to (such as policies covering email and internet use)*
- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking*
- *Investigating complaints*
- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*
- *Monitoring staff conduct, disciplinary matters*
- *Promoting Council services*
- *Improving services*

Personal data - means any information relating to an individual that can be used directly or indirectly to identify the person. This may be an employee, job applicant, current and former employee, clients, suppliers, members of the public, Council service users, residents, correspondents. Personal data we gather may include: individuals' names and contact details, date of birth, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV, contact details, correspondence, emails, council records or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual. Any use of sensitive personal data should be strictly controlled in accordance with this policy.

5. Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Parish Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual

- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

The Data Protection Officer's responsibilities:

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Assisting with data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, council members and other stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know what data is being held on them by Foxton Parish Council.
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Officers

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

6. The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our General Protection Privacy Notice and Privacy Notice for Employees, Councillors and Role Holders can be found on our website at www.foxtonparishcouncil.gov.uk or requested from the Parish Clerk at clerk@foxtonparishcouncil.gov.uk.

The privacy notices:

- Set out the purposes for which we hold personal data on customers, employees, residents and service users
- Highlight that our work may require us to give information to third parties such as the District and County Council and professional advisers.
- Provide that service users and correspondents have a right of access to the personal data that we hold about them

7. Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

8. Children

The Parish Council will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

9. Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Local Council Public Advisory Service.

10. Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

11. Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

12. Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Data should be regularly backed up
- Data saved directly onto mobile devices such as laptops, tablets or smartphones should be password or finger print protected in case they are lost or stolen
- All servers containing sensitive data must be approved and protected by security software and strong firewall

13. Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

14. Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. Who may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

15. Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

16. Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training should cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

17. Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation.

The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	Foxton Parish Council
How is it collected?	Email, written correspondence, internet contact form and by phone
Why is it being collected?	To transact Parish Council business

How will it be used?	Only as necessary to transact Parish Council business – see Privacy Notices for more detail
Who will it be shared with?	Parish Councillors and any data controllers listed under our General Privacy Notice
Identity and contact details of any data controllers	Foxton Parish Council clerk@foxtonparishcouncil.gov.uk
Retention period	In accordance with our Retention Policy

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

18. Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

19. Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

20. Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

21. Monitoring and compliance

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to. We take compliance with this policy very seriously. Failure to comply puts both you and Foxton Parish Council at risk.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

22. Changes to this policy

We keep this Privacy Policy under regular review and we will place any updates on our web page at www.foxtonparishcouncil.gov.uk. This Policy was last updated in May 2018.

23. Contact Details

Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller:
Foxton Parish Council
Email: clerk@foxtonparishcouncil.gov.uk

The Data Protection Officer:
CAPALC
PO Box 181, St Ives, PE27 9DR
Tel: 01480 375 629
Email: accounts@capalc.org.uk