ST STEPHEN PARISH COUNCIL

DATA PROTECTION PRIVACY STATEMENT

1. Back ground

This Statement takes account of UK and EU law and conventions and specifically to address the General Data Protection Regulations 2018 (GDPR). St Stephen Parish Council is aware of its obligations under the Data Protection legislation and GDPR and has undertaken a number of actions to comply:

2. Data Audit

A comprehensive audit of all data held by the Council has been undertaken to identify all individuals where personal data is collected, recorded and processed by the Council or a contractor acting on behalf of the Council. The audit covered employees, volunteers, service users, customers, suppliers and contractors. The audit also identified where data was being kept, in what format and why the data was being collected and used.

The opportunity was also taken to review the technical and operational security measures in place to prevent or minimise unintentional or malicious access to, or loss of, personal or confidential organisational data. A report is available from an IT specialist setting out the technical safeguards that are in place.

We will undertake an audit of all types of data collection, recording and processing taking place on an annual basis. We will review the reasons for the data being obtained and justify why this should continue or make a decision it will no longer be obtained.

Similarly, we will review the way in which the data is stored and processed to ensure all appropriate safeguards are in place and security/confidentiality measures are effective. We will:-

- carry out a risk assessment of data systems and act on the results
- maintain up-to-date security systems (for example, using firewalls and encryption technology)
- restrict access to personal data to only those who demonstrate that they need it
- train staff on data security
- review data security regularly.

3. Policies, Guidance & Awareness

To underpin compliance with the legislation and GDPR the Council has reviewed and revised its Data Protection Policy and has agreed a Records Management Policy that sets out the legal framework and timescales for keeping data and best practice with regard to storing data and

destroying material when no longer required**.** A copy of these policies are available on the Council's website and/or by contacting the Clerk in writing at the address below.

Guidance has been issued to employees and Councillors on Data Protection and their rights and obligations, as well as Guidance on Data Operational Security so that everyone operates in a way and follows procedures that safeguards personal data and prevents accidental or malicious disclosure. An external consultancy has been commissioned to advise the Council on the implementation of the GDPR and to provide ongoing monitoring and quality assurance input. The Council's policies and contract documentation have been revised to included information and guidance on data protection.

Councillors and employees who work from home whether on an ad hoc basis or more generally have been asked to sign a data protection declaration to say that any personal data in their possession is kept confidential and secure.

4. Informing individuals and seeking consent (Privacy Notices)

Councillors have been informed of what personal data is being held on them by the Council or third parties and have been asked to check the accuracy of the data and been given the opportunity to update the personal data. The reasons why their data is being collected recorded and used has been explained and their new rights outlined. Individual Councillors have been given the opportunity to challenge why their data is being kept, how it is being used and who has access to their data. Specific consent has been obtained from the individuals where there are no legal requirements to collect, record and process their data.

Employees of the Council (and applicants for job vacancies) have been informed of what personal data is being held on them by the Council or third parties and have been asked to check the accuracy of the data and been given the opportunity to update the personal data. The reasons why their data is being collected recorded and used has been explained and their new rights outlined. Individual employees have been given the opportunity to challenge why their data is being kept, how it is being used and who has access to their data. Specific consent has been obtained from the individuals where there are no legal requirements to collect, record and process their data.

Volunteers, where used will similarly have been informed of any personal data that is being held on them and why this is required and asked to check for accuracy. Volunteers also have the same rights as employees and can challenge the Council. Specific consent has been obtained from the individuals where there are no legal requirements to collect, record and process their data.

Allotment Holders personal data is kept for the management of allotments and payment of fees and existing and new allotment holders have been informed of what personal data is being kept and why, been given the opportunity to check the personal data and informed of their rights.

Community Engagement where personal data is obtained from those attending events, including Council Meetings and consultation events, will have information made available to be given to, or to alert, participants with regard to their rights under data protection and to safeguard their privacy but bearing in mind these are public events and the media may use personal details for publication in the media including social media.

Suppliers to the Council in the main suppliers personal data is not held by the Council as suppliers contact details are usually in the public domain as part of their business activities. The Council has however checked with suppliers that those details are correct.

Contractors to the Council fall into two groups – those providing a time limited service such as building works or maintenance where their contact details will be as per those of Suppliers and then Contractors who are contracted to provide a specific service to the Council such as HR, Health & Safety, pensions or payroll services. Those contractors providing a specific service may have access to the personal data of Councillors, employees and volunteers, and in some cases of service users.

Where this occurs the Council In each case we will have verified that the Contractor has a Data Protection and/or Privacy Policy, complies with the principles of the Data Protection Act, has adequate safeguards and security protocols and only uses the personal data for the purpose we have contracted the Contractor to provide.

Premises Users/Leaseholders of premises personal data is kept for the management of premises bookings or the operation of leases and the payment of fees and existing and new users and lessees have been informed of what personal data is being kept and why, been given the opportunity to check the personal data and informed of their rights.

5. Access to Data

A request for access to any personal data that relates to an individual will be made by a written request using the Data Access Request form and the originator's details will be verified. The request must be submitted to the clerk in writing at the address. There are no fees chargeable for this.

Employees consent will be obtained where the Council is making personal data /information available to those who provide services to the Council (such as HR advisors), regulatory authorities, governmental or quasi-governmental organisations.

Where contractors are used to obtain, record, store or process personal data on behalf of the organisation, that service provider will only be commissioned or have a contract renewed if they meet data protection quality assurance standards set by us, so that they can demonstrate compliance with the DPA and GDPR. There may be certain circumstances where a person's consent cannot be obtained or is not legally required. Before releasing personal data to external organisations (including the police) the Council will seek to obtain legal advice on its obligations and where necessary ask for a court order or a Magistrates warrant before release of personal information about employees, customers or others.

The Council's policy is to provide copies of all data that the organisation is obliged to disclose within 20 working days of receipt of a request being received by the Clerk.

The Council considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect us to be obliged to comply with a further request before a year has elapsed unless there are exceptional circumstances.

Where we have requested an employment reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed, it is our policy that it would normally be unreasonable to disclose such a reference to others unless the consent of the person who gave the reference is obtained.

6. Breach of data protection policy or legal requirements

Any suspected or actual breach of data or privacy whether direct or indirect, malicious or unintentional will be reported immediately to the Clerk and the ICO (Information Commissioner's

Office) informed. The organisation will implement its Contingency Plan in order to immediately protect personal data and resolve the cause of the breach. We will consider any serious breach of the policy and data protection rules to be a serious incident and this will be investigated thoroughly and measures taken to remedy the situation and action taken against those felt to be negligent.

7. Protection against detriment

Employees, volunteers and service users will not suffer any detriment, or penalty for challenging the personal data we hold on them or the processes involved, for making subject data access requests or refusing consent to the obtaining, recording or processing of the individual's personal data. Anyone concerned about the legal status or ethical use of anyone's personal data by the organisation should report this immediately to the Clerk.

8. Evaluation and review

This Policy will be regularly reviewed by the Council to ensure its effectiveness and compliance with the law and any necessary changes agreed and implemented in consultation with all staff.

9. Data Protection Responsibility

The Council has appointed the Clerk to be responsible for all data protection matters. To give an independent element to the role the Clerk will be supported by CP Associates who will also operate a helpline for any stakeholders with regard to the Council's implementation of GDPR or who have any queries in relation to their rights under the regulations. CP Associates will also be involved in the investigation into any breaches. Any comments or questions about the operation of this Policy should be addressed in writing to by contacting the Clerk at the address below.

12.Adoption

This Policy was adopted by resolution of St Stephen Parish Council at their meeting on 14th June 2018.

June 2018

St Stephen Parish Council
The Parish Centre
Station Road
Bricket Wood
St Albans
Herts
AL2 3PJ