STOURPAINE PARISH COUNCIL

Privacy Policy and Freedom of Information Policy

Adopted: 21st May 2018
Updated: 17th October 2019

Contents

1. Introduction

Stourpaine Parish Council ("the Council") is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) from 25th May 2018, which supersedes the Data Protection Act.

The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the GDPR and that the Council remains committed to protecting and respecting the privacy of all who provide their data.

For the purpose of the GDPR, the data controller is:

Stourpaine Parish Council, 1 North Mead Farm, Front St., Portesham, Weymouth Dorset DT3 4FY.

2. Statement of Policy

In order to operate efficiently, the Council has to collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the GDPR to ensure this. The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly. Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by public authority acting in the public interest, out of contractual necessity or on a lawful basis.

The Council will seek the consent of individuals and companies to hold their personal data, where possible to do so. Records of those consenting will be kept.

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Privacy Policy

The Council is committed to protecting and respecting the privacy of everyone and of ensuring it is fully compliant under the General Data Protection Regulation.

This policy (together with any other documents referred to within it) sets out the basis on which any personal data the Council collects, or is provided to it, will be processed. The following policy sets out the Council's practices regarding the collection and processing of personal data and how the Council treats it.

a) Personal Data the Council may collect:

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including GDPR and other legislation relating to personal data and rights such as the Human Rights Act.

b) Data Controllers:

Stourpaine Parish Council is the data controller for all data collected.

Other data controllers the Council works with:

- Parish, District and County Councillors
- Local groups and organisations (Volunteers/Allotment holders)
- Dorset Council
- HMRC and other Central Government bodies
- Charities
- Contractors

The Council may need to share personal data that it holds with them so that they can carry out their responsibilities to the Council. If the Council and the other data controllers listed above are processing data jointly for the same purposes, then the Council and the other data controllers may be "joint data controllers" which means the Council and the other data controllers are all collectively responsible for the data. Where each of the parties listed above are processing data for their own independent purposes then each of them will be independently responsible.

c) What data does the Council process?

The Council will process some, or all of, the following personal data where necessary to perform its tasks (see also the Council's Information Audit):

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by the Council, or where you provide them to the Council, the Council may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a Council venue, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

- The personal data the Council processes may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

d) How the Council uses sensitive personal data

- The Council may process sensitive personal data in order to comply with legal requirements and obligations to third parties.
- The Council needs to have further justification for collecting, storing and using this type of personal data.
- The Council may process special categories of personal data in the following circumstances:
  - In limited circumstances, with explicit written consent.
  - Where the Council needs to carry out its legal obligations.
  - Where it is needed in the public interest.
- Less commonly, the Council may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect an individual's interests and they are not capable of giving consent, or where the information is already public.

e) Do the Council need consent to process sensitive personal data?

- In limited circumstances, the Council may approach individuals for written consent to allow it to process certain sensitive personal data. If the Council do so, the Council will provide full details of the personal data that the Council would like and the reason the Council need it, so that the individual can carefully consider whether they wish to consent.

f) The Council will comply with data protection law, this says that the personal data the Council holds about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that the Council has clearly explained and not used in any way that is incompatible with those purposes.
- Relevant to the purposes the Council have stated and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes the Council have stated.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect personal data from loss, misuse, unauthorised access and disclosure.

g) The Council use your personal data for some or all of the following purposes:

- To deliver public services, including to understand individuals needs to provide the services that they request and to understand what the Council can do for the individual and inform them of other relevant services;
- To confirm identity to provide some services;
- To contact by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help the Council to build up a picture of how it is performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for law enforcement functions;
- To enable the Council to meet all legal and statutory obligations and powers including any delegated functions;

- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the Council;
- To maintain the Council's own accounts and records;
- To seek views, opinions or comments;
- To notify of changes to the Council's facilities, services, events and staff, councillors and other role holders;
- To send communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the Council
- To allow the statistical analysis of data so the Council can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

h) What is the legal basis for processing your personal data?

The Council is a public authority and has certain powers and obligations. Most of the personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the Council's services. The Council will always take into account the interests and rights of the individual. This Privacy Policy, and the Privacy Notices, the Council displays and distributes sets out the rights and the Council's obligations to each individual. The Council may process personal data if it is necessary for the performance of a contract, or to take steps to enter into a contract. An example of this would be processing data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy. Sometimes the use of personal data requires consent, the Council will first obtain consent to use that data.

i) Sharing personal data

This section provides information about the third parties with whom the Council may share personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to the individual directly for the manner in which they process and protect personal data. It is likely that the Council will need to share data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the Council works with";
- Our agents, suppliers and contractors. For example, the Council may ask a commercial provider to publish or distribute newsletters on its behalf, or to maintain its database software;
- On occasion, other local authorities or not for profit bodies with which the Council are carrying out joint ventures e.g. in relation to facilities or events for the community.

j) How long do the Council keep personal data?

The Council will keep some records permanently if the Council are legally required to do so. The Council may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support

HMRC audits or provide tax information. The Council may have legal obligations to retain some data in connection with its statutory obligations as a public authority. The Council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). The Council will retain some personal data for this purpose as long as the Council believe it is necessary to be able to defend or pursue a claim. In general, the Council will endeavour to keep data only for as long as it is needed. This means that the Council will delete it when it is no longer needed.

k) Individual rights and their personal data

Individuals have the following rights with respect to personal data:

When exercising any of the rights listed below, in order to process a request, the Council may need to verify identity for security. In such cases the Council will need the individual to respond with proof of identity before they can exercise these rights.

i) **The right to access personal data the Council holds -** At any point an individual can contact the Council to request the personal data it holds as well as why it has that personal data, who has access to the personal data and where it has obtained the personal data from. Once the Council have received a request it will respond within one month. There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

ii) **The right to correct and update the personal data the Council holds -** If the data the Council holds is out of date, incomplete or incorrect, individuals can inform the Council and the data will be updated.

iii) **The right to have personal data erased -** If an individual feels that the Council should no longer be using their personal data or that it is unlawfully using it, they can request that the Council erases the personal data it holds. When the Council receive a request, it will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because the Council needs it to comply with a legal obligation).

iv) **The right to object to processing of personal data or to restrict it to certain purposes only -** Individuals have the right to request that the Council stops processing their personal data or ask it to restrict processing. Upon receiving the request, the Council will contact the person concerned and let them know if it is able to comply or if it has a legal obligation to continue to process the data.

v) **The right to data portability -** Individuals have the right to request that the Council transfers some of their data to another controller. The Council will comply with a request, where it is feasible to do so, within one month of receiving it.

vi) **The right to withdraw consent to the processing of data to which consent was obtained -** Individuals can withdraw their consent easily by telephone, email, or by post (see Contact Details below).

vii) **The right to lodge a complaint with the Information Commissioner's Office.** To lodge a complaint, individuals can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

l) Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. The Council's website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

m) Further processing

If the Council wish to use personal data for a new purpose, not covered by the Privacy Policy or Privacy Notice, then the Council will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, the Council will seek prior consent to the new processing.

n) Changes to the Policy

The Council keep this Privacy Policy under regular review and the Council will place any updates on the Council's website at http://www.stourpaine.info/parishcouncil/

4. Subject Access Request (SAR)

- The Council will inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted.
- At any point an individual can contact the Council to request the personal data it holds as well as why it has that personal data, who has access to the personal data and where the Council obtained the personal data from. Once the Council has received a request it will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.
- Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.
- The Council will implement standards to respond to SARs, including a standard response.

Upon receipt of a SAR the Council will;

- Verify whether it is the controller of the data subject's personal data. If it is not the controller, but merely a processor, the Council will inform the data subject and refer them to the actual controller.
- Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- Verify the access request to ensure it is sufficiently substantiated. Ensure it is clear to the data controller what personal data is requested and If not request additional information.
- Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, the Council may refuse to act on the request or charge a reasonable fee.
- Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
- Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.
- Respond to a SAR within one month after receipt of the request, If more time is needed to respond to complex requests, an extension of another two months will be taken, this will be communicated to the data subject in a timely manner within the first month;
- If the Council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
- If a SAR is submitted in electronic form, any personal data will be provided by electronic means if possible.
- The Council will include as a minimum the following information in the SAR response:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;
- Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with the Information Commissioners Office ("ICO");
- If the data has not been collected from the data subject: the source of such data;
- The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Provide a copy of the personal data undergoing processing.

5. Data Protection Impact Assessments (DPIAs)

The Council will carry out Data Protection Impact Assessments, (DPIAs), when it is necessary. The Council will consider the following:

- Whether or not to carry out a DPIA;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.
- The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. This might include using CCTV to monitor public areas. A checklist is provided by NALC to help Councils assess the need for a DPIA and provides a springboard for some of the issues to consider in more detail.

6. Cybersecurity

Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

The main storage location for data is the Clerk's laptop, memory sticks in locked storage, and a locked filing cabinet, and this is protected in the following way;

- Antivirus software
- Complex passwords of 8 or more characters secure all access
- Account lock out for 5 or more incorrect password in 30 minutes

7. Security Incident Response

The Council takes any breach of data security seriously and in the event of such a breach the following response plan will be followed:

A data security breach is defined as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of which are:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen
- Loss of availability of personal data.

In the event of a breach the Clerk is to be notified immediately, and in his/her absence the Chairman should be informed. The Clerk and the Councillors are instructed to report any breaches immediately they suspect one may have occurred. An assessment will be made on the severity of any potential breach. Decisions are to be made by the Clerk after consultation with the Councillors. These decisions will include but are not limited to: notifying the correct supervisory bodies and the individual involved in the breach.

If after investigating the incident it is confirmed that a personal data breach occurred, the Council will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then the Council will notify the Information Commissioners Office (ICO). Any notifications to the ICO will be done not later than 72 hours after the breach was identified. The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows the Council to provide the required information in phases, as long as this is done without undue delay. The Council will always prioritise the investigation, give it adequate resources, and expedite it urgently.

The Clerk in conjunction with the Chairman will decide if the breach is notifiable after assessing both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. In such cases, the Council will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them, therefore allowing them time to take steps to protect themselves from the effects of a breach. The Council will provide them with a description of the likely consequences of the personal data breach; and what measures are being taken, or proposed to be taken, to deal with the breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the decision is taken not to notify individuals, the Council will still notify the ICO unless the breach is unlikely to result in a risk to rights and freedoms. However, if a decision is made not to inform the ICO then that decision will be documented. As with any other breach of procedures or security incident officers will thoroughly investigate to ascertain whether the breach was a result of human error or a systemic issue. It will then be determined the best way to ensure how a recurrence can be prevented, whether this is through better processes, further training or other corrective steps.

8. Freedom of Information Policy

The Council is committed to complying with the provisions of the Freedom of Information Act 2000 and associated legislation. This provides a general entitlement to information that the Council holds to any person subject to exemptions and conditions laid down by law.

Scope

This policy applies to all recorded information the Council holds regardless of how it was created or received. It applies regardless of the media the information is stored in whether the information may

be on paper, held electronically or as an audio recording. The Act is fully retrospective. Dealing with requests the Council offers advice and assistance to anybody who wishes to make a Freedom of Information (FOI) request. The Council is committed to dealing with requests within the statutory timescales of no more than 20 working days. This can be extended in specific circumstances on legal advice. However, the Council is committed to providing a prompt service.

The Council will claim exemptions as appropriate whilst maintaining a commitment to openness, scrutiny and the public interest and will inform the FOI applicant when exemptions have been applied. Where appropriate, requests in writing will be treated as Freedom of Information requests. There is no need for requests to indicate they are made under the Act. The Council reserves the right to refuse requests where the cost of supply of the information would exceed the statutory maximum (see section 12 of the Act.).

Adopting and Maintaining Publication Schemes

The Council has adopted an Information Publication Scheme (attached at Appendix A) and is committed to updating and maintaining it to keep it current and relevant. The Publication Scheme contains many of the documents, policies, plans and guidance which are usually asked for and much more. Material contained within the publication scheme, and a copy of the scheme itself, is readily available. Where charges are applied these are stated in the Scheme. The scheme can also be accessed via the website. The Clerk will give advice and assistance on how to use the scheme as appropriate. This scheme is reviewed an updated on an annual basis.

Responsibilities

The Clerk is responsible for ensuring that any request for information is dealt with under the Act and in compliance with this policy. The Clerk is also responsible for good information handling practice and implementing records management policies and procedures as appropriate. The Council will carefully consider its responsibilities under GDPR before releasing any personal data about living individuals, including current and former officers, current and former Council Members, and users of the Council's services.

Contact Details

For advice and assistance please contact the Parish Council:

Stourpaine Parish Council
1 North Mead Farm
Front St
Portesham
Weymouth
Dorset
Tel: 07814016971
Email: clerk@stourpaine.org.uk
Website: http://www.stourpaine.info/parishcouncil

Further advice and information, including a full list of exemptions and advice on the public interest test, is available from the Information Commissioner's Office www.ICO.org.uk.

9. Associated Documents

Other documents related to both the Data Protection and Freedom of information policy are:

- Publication Scheme (attached at Appendix A)
- Risk Management Policy
- Privacy Notice

- Information Audit

Appendix A

INFORMATION AVAILABLE FROM STOURPAINE PARISH COUNCIL ADOPTED AT COUNCIL [ ] October 2019

Costs are listed at the end

INFORMATION TO BE PUBLISHED	HOW THE INFORMATION CAN BE OBTAINED
Class 1 – Who the Council are and what the Council do	
Who's who on the Council and Groups	Website Hard copy from Clerk Noticeboards
Contact details for Parish Clerk and Council members	Website Hard copy from Clerk Noticeboards
Staffing Structure	Only employee is Clerk
Class 2 What the Council spend and how the Council spend it	
Current and previous financial year	Website Hard copy from Clerk
Annual return form	Website Hard copy from Clerk
Finalised budget	Website Hard copy from Clerk
Precept	Hard copy from Clerk
Grants given and received	Hard copy from Clerk
Class 3 – What the Council's priorities are and how the Council are doing	
Minutes of Meetings	Website Hard copy from Clerk
Class 4 How the Council make decisions	
Calendar of meetings	Website Hard copy from Clerk
Agendas of Meetings	Website Hard copy from Clerk Most recent – Noticeboards
Minutes of Meetings	Website Hard copy from Clerk Last draft Minutes – Noticeboards
Reports presented to Council meetings	Hard copy from Clerk
Responses to consultation papers	Hard copy from Clerk Website
Responses to planning applications	Dorset for You website
Class 5 – The Council's policies and procedures	
Policies and procedures for conduct of council business including Code of Conduct, Standing Orders and Financial Regulations	Website Hard copy from Clerk
Class 6 – Lists and Registers	
Assets register	Website Hard copy from Clerk

SCHEDULE OF CHARGES

£1 for the first single-sided A4 sheet of each request. 20p for each subsequent item. Where copies are mailed, an additional £2 plus appropriate postage. The Chairman is authorised to waive any fee if it is considered appropriate. For research requests requiring more than the mandatory nominal £450, an hourly rate of £25 will apply – this figure to be subject to review.

Parish Clerk, Marianne Wheatley
1 North Mead Farm
Front St
Portesham
Dorset DT3 4FY
E-mail: clerk@stourpaine.org.uk