Stratfield Saye Parish Council

IT and Data Policy

Version
201805

Procedure Owner
Clerk to the Council

Approval Body
Stratfield Saye Parish Council

Last Review Date
May 2018

Next Review Date
May 2019

Summary

Stratfield Saye Parish Council ("SSPC") is a civil local authority found in England and is the lowest tier of local government authorised under the Local Government Act 1972. Its aim is to provide effective, efficient and accountable local government for the parish, enabling residents to be involved in the life of the community and its future development.

This Policy sets out the principles determining how SSPC handles personal data in accordance with the General Data Protection Regulation ("GDPR"). It includes details on what types of personal data that SSPC expects to hold.

The GDPR (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation was adopted on 27th April 2016 and becomes enforceable from 25th May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

Scope

This Policy details the requirements that the Council, the Councillors and the Clerk are required to undertake to comply with GDPR requirements.

This Policy does not cover the activities of Councillors and the Clerk when they acting in a personal capacity.

Roles and Responsibilities

The Council act in the capacity of data controller, in that they set the Policy and determine the rules under which all covered relevant parties operate.

The Clerk will act as the data processor in that the Clerk will, in most circumstances, be in possession of the personal data that the Council holds. Notwithstanding this, all Councillors must also ensure that they comply with this policy in all aspects, e.g. email usage.

The Council will appoint a Data Protection Office (DPO). This cannot be a Councillor.

GDPR Principles

There are 7 high level principles behind the GDPR. These are:

Lawfulness, fairness & transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Storage limitation	Personal data shall be 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
Integrity & confidentiality	Personal data shall be 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Personal Data

The personal data that SSPC holds is limited in scope and is likely to be limited to names and contact details. A list of various possible data types in included in the table below, together with the likelihood that SSPC would possess each type.

Name	SSPC will collect personal contact data supplied by the Parish for (i) keeping the community updated on Parish news and developments; or (ii) for specific projects (e.g. Broadband provision
Personal – Address	SSPC will collect personal contact data supplied by the Parish for (i) keeping the community updated on Parish news and developments; or (ii) for specific projects (e.g. Broadband provision
Personal – Email	SSPC will collect personal contact data supplied by the Parish for (i) keeping the community updated on Parish news and developments; or (ii) for specific projects (e.g. Broadband provision
Personal – Telephone	SSPC will collect personal contact data supplied by the Parish for (i) keeping the community updated on Parish news and developments; or (ii) for specific projects (e.g. Broadband provision

Date of Birth	SSPC are highly unlikely to need this information
Emergency Contact	SSPC are highly unlikely to need this information
IP address	SSPC are highly unlikely to need this information
Credit Card Details	SSPC are highly unlikely to need this information
National Insurance Number	SSPC are highly unlikely to need this information
Bank Account Information	SSPC will hold bank account information provided to it by Councillors and contractors for the payment of expenses and settlement of invoices.
Images	SSPC are highly unlikely to need this information for any individual (e.g. for an ID card). Photographs taken at SSPC events are deemed to be in public, and no additional consent is needed to use the images on the SSPC website or social media pages. SSPC will, however, entertain requests to remove, edit and/or crop images should such requests be received. Where the request involves a minor then SSPC would normally agree to the request.
Voice Recordings	SSPC are highly unlikely to need this information
Passport	SSPC are only likely to need this information to ensure the Clerk or other possible staff have the right to work in the UK.
Driving Licence	SSPC are highly unlikely to need this information
Criminal Convictions / Offences	SSPC will only hold this information in relation to the Clerk.
Education & Training	SSPC will retain a record of training undertaken by Councillors.
CV	SSPC may receive CVs from applicants for the role of Parish Clerk.
References	SSPC may seek references for applicants who have applied for the role of Parish Clerk. The names of the referees will have been supplied by the candidate(s), who will be required to seek consent from the referees for SSPC to contact them.
Annual appraisals	SSPC are highly unlikely to need this information
Employment Status	SSPC will only hold this information in relation to the Clerk.
Work permit	SSPC will only hold this information in relation to the Clerk.
Leave	SSPC are highly unlikely to need this information
Pension details	SSPC are highly unlikely to need this information
Hobbies / Social	SSPC are highly unlikely to need this information
Family	SSPC are highly unlikely to need this information. Any data collected in other categories is expected to be for adults only. It is not within the normal business of the Council to require personal data on children, and as such it is not likely this data will ever be held.
Sexual orientation	SSPC are highly unlikely to need this information
Ethnicity	SSPC are highly unlikely to need this information
Health	SSPC are highly unlikely to need this information
Biometrics (fingerprint, retinal scan, DNA)	SSPC are highly unlikely to need this information
Trade Union Membership	SSPC are highly unlikely to need this information
Political opinions	SSPC are highly unlikely to need this information
Religion	SSPC are highly unlikely to need this information

Electoral Register

The Electoral Register for SSPC is maintained by Basingstoke and Deane Borough Council ("BDBC"). A version of the full Register is provided to the Clerk by BDBC when the Clerk makes a written request for it. As such, BDBC will be treated as the data owner, and therefore any issues regarding individual rights will be addressed by BDBC. Once received, the Register itself will be subject to the data security provisions of the GDPR.

There are legal restrictions on who is allowed to receive a copy of the full register, and what they are permitted to do with this. As such, these restrictions will apply in this situation in addition to any requirements under GDPR and this Policy.

Note that candidates for election to the Council are permitted to receive a copy of the full register. This is provided to the candidate by the Electoral Services team at BDBC, and not by the Clerk or SSPC. BDBC will inform the candidate of the restrictions and requirements in relation to their handling of the Full Register.

Where a sitting Councillor is seeking re-election, they are treated as a candidate in terms of receiving the register from BDBC, and are not in scope of this policy.

Lawful Basis for Processing

There are six lawful bases set out in Article 6 of the GDPR. These are:

(a) Consent: the individual has given clear consent for SSPC to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract SSPC have with the individual, or because they have asked SSPC to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for SSPC to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for SSPC to perform a task in the public interest or for SSPC's official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for SSPC's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply as SSPC are a public authority processing data to perform SSPC's official tasks.)

In most cases the data will be collected with the consent of the person involved. There may be circumstances under which SSPC may require information for a specific purpose. For example, data requested for the Parish for the purposes of planning Broadband installation would be covered under basis (b).

Individual Rights

Individuals have the following rights under GDPR:

Right to be Informed

This right encompasses the obligation to provide "fair processing information", and emphasises the need for transparency over how the personal data is used, and must be provided in a concise, transparent, intelligible and easily accessible manner.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

A privacy notice will be published on the Council's website.

Right of Access

An individual is entitled to obtain access to their personal data and to get confirmation that their data is being processed.

The data must be provided free of charge, although a fee may be charged if the request is manifestly unfounded or excessive, or if it is repetitive. The fee must be based on the administrative cost of providing the information.

Data must be provided without delay, and within one month of the receipt.

All requests must be made in writing or via email to the Clerk.

Right to Rectification

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. If the data has been supplied to a third party, SSPC will inform the third party of the correction, and notify the individual to whom the data has been provided.

Right to Erasure

This is commonly referred to as "the right to be forgotten". SSPC will erase data:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child

It is permitted to refuse a request where in certain circumstances under GDPR. SSPC will review requests in the context of the permitted exemptions.

Right to Restrict Processing

Individuals have the right to stop the processing of data. SSPC is still permitted to store the data, but must not process it further. GDPR permits SSPC to store enough information to endure this request is respected in the future.

Right to Data Portability

This right allows an individual to require SSPC to send data to another organisation for processing. The data that SSPC holds and what it uses it for makes this a highly unlikely scenario.

Right to Object

This right covers direct marketing, profiling and research, and is it not expected to be pertinent for SSPC.

Right Related to automated decision making including profiling.

This is not relevant for SSPC.

Accountability and Governance

Contracts

Where SSPC engages a contractor to process data, it will ensure it has written contract that covers the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Documentation

Data protection by design and default

Whenever SSPC receives data for a new purpose, or changes it method of processing, the data Protection Officer will review the process to ensure that the privacy and data protection requirements are assessed.

Data Protection Impact Assessments ("DPIA")

SSPC is required to conduct a DPIA (also known as Privacy Impact Assessments or PIAs) whenever it undertakes a new project. Data security must be an integral consideration in any project design.

Data Protection Officer ("DPO")

The latest guidance is that, despite being a public body, as a Parish Council that SSPC is not required to appoint a Data Protection Officer, but may do so if they choose. SSPC shall not be making an appointment to this role.

Codes of Conduct and Certification

There is no requirement for SSPC to sign up to codes of conduct or certification, and SSPC will not be seeking certification.

Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The ICO has previously produced guidance to assist organisations in securing the personal data they hold. We are working to update existing guidance to reflect GDPR provisions and once completed, this section will expand to include this information.

International Transfers

SSPC will use a UK based company for hosting its website. Any backup or Cloud services will be with UK based companies.

Data breaches

A personal data breach means a breach of security leading to 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.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The DPO must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, SSPC must also inform those individuals without undue delay.
SSPC should ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not SSPC need to notify the relevant supervisory authority and the affected individuals.

SSPC must also keep a record of any personal data breaches, regardless of whether SSPC are required to notify.

Fines for breaches are up to an upper limit of €20 million, or 4% of an organisation's annual turnover, whichever is the higher.

The DPO is required to report any data breaches to the ICO within 72 hours of the breach being detected. Should the DPO be unavailable in this timescale then the following are required to ensure the notification is made:

1. The Chair of SSPC
2. The Vice-Chair of SSPC
3. Any other Councillor. Councillors must liaise to ensure that one Councillor takes responsibility for in this case.

Exemptions

GDPR allows national governments to introduce derogations to the GDPR in certain circumstances. The types of permitted exemptions are not expected to impact SSPC.

Applications

GDPR requirements have been not finalised by the Information Commissioner's Office ("ICO"). When the requirements are produced this section will be reviewed.

Children

SSPC do not hold, nor are expected to hold, data relating to children in the normal course of its business. Should this change then the DPO will assess the data handling of such data in the context of the GDPR requirements.

Data Security and IT set up

This section details how SSPC will handle data in terms of data security and associated IT set up.

Paper Records

All Councillors and the Clerk are responsible for ensuring that all paper records in their possession are securely stored.

Electronic Records

On no account should data be stored on removable drives, e.g. USB sticks, due to the possibility of loss or theft. Where Councillors or the Clerk need to store data, this should be on a password protected PC / Laptop.

Speakers at Council Meetings

The Council supports the principles of openness and transparency in the way it conducts its meetings. Please refer to the section "Protocol for Reporting at Meetings" within the Standing Orders of the Council for further information and requirements.

Where a member of the public speaks due the Open Forum session of a Council meeting, the person's name will not be recorded in the minutes.

IT Set up

SSPC will apply for a gov.uk domain name. This will be with a UK based web host, who will also handle all of the email traffic. The website will be used to provide information on Council events, advertise meetings, and act as a reference for the local community by supplying relevant public data.

Emails

The Clerk and each Councillor will each have their own email address on a gov.uk domain. This will be used exclusively for any correspondence on Council business. Private email addresses are not permitted to be used. All email data will be archived.

Where the Clerk or a Councillor sends out an email to a group of recipients to convey information on Council events or similar, they must ensure that all recipients are included in the BCC field, and not the CC field.

Councillors and the Clerk are not permitted to send any data to their personal email addresses.

Where a Councillor is contacted on their personal email for Council business, they are to forward the email to their Council email address and reply to the correspondent from their Council address, making correspondent aware that this is the email they should use going forward.

Social Media

The Council may publish announcements and information on social media. Where a member of the public responds or reacts to any such posting (e.g. adding a comment or "liking" a post), then they are deemed to consent to such information that they post to be public and shall be responsible for such information.

Where a request to be forgotten is received, the Council may not be able to delete the requestor's interaction, and in such cases the requestor shall be responsible for removing their interactions.

Third Party Suppliers

Where the Council engages a Third Party to supply goods and / or services to the Council, the Clerk shall review whether the Council need to supply personal data to the supplier. Should this be the case, the Clerk will request a copy of the GDPR policy from the supplier so that the DPO can ensure that their data handling is of the required standard for GDPR compliance.

No data shall be supplied to the Third Party until the DPO is satisfied that the Third Party's policy is sufficient.

The Clerk will record what information is supplied so that:

- Should a request to be forgotten be received, the Third Party can be instructed to delete the information.
- Where the data is no longer required, the Third Party can be instructed to delete the personal data.

In both cases the Clerk will confirm to the DPO that confirmation has been received from the Third Party that the data has been deleted.

Data Encryption

Where Councillors and / or the Clerk need to share personal data, this must be done in a secure manner. This will include sending data in an encrypted or password protected manner. Data can only be sent to a Councillor's email address on the gov.uk domain, and Councillors are prohibited from forwarding any email correspondence to their personal email.

Data Retention

Where personal data is no longer required for the purpose for which it was collected, it shall be deleted.

Exceptions apply for areas such as HMRC where record retention is required for several years, or where there is, or likely to be, a legal claim or for other purposes.

SSPC may need to keep some personal data so that SSPC can deal with any complaints they might receive about the services they provided.

SSPC may also keep the personal data it holds about an individual when that individual leaves the organisation's employment. It will need to retain enough data to enable the organisation to deal with, say, providing references. However, personal data that is unlikely to be needed again will be removed from SSPC's records, for example the individual's emergency contact details or previous addresses.

Privacy Notice

SSPC will include a privacy notice on its website detailing its data handling principles. A copy will also be affixed to the public noticeboards in the Parish.

Employment Data

SSPC employs the Clerk to the Council, and as such SSPC are required are to:

- Seek the consent of the Clerk to process personal information.
- SSPC will provide to the Clerk the source of data, who will hold the data and for how long it will be stored

Where data is required to be held for other means, e.g HMRC records, it may not be possible for the Clerk to enforce the right to be forgotten.