Data Protection Policy

Statement of intent

Selwood Parish Council (SPC) is committed to a Policy of protecting the rights and privacy of individuals. In order to do this, we must comply with the General Data Protection Regulation and complementary Data Protection Act 2018, which, which impose responsible behaviour upon those using PD. We need to process certain types of Personal Data (PD) in order to carry on our work of managing SPC. We are committed to processing this PD securely and recognise the risks to individuals of identity theft and financial loss if PD is lost or stolen. Furthermore, we regard the lawful and correct processing of PD as essential for the success of our organisation and for maintaining the confidence of everyone we deal with.

Purpose

The DPA and GDPR govern the use of PD, which can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs. This document explains how SPC complies with the DPA and GDPR in handling PD.

The Information Commissioner's Office (ICO) is responsible for implementing and overseeing the DPA. The Policy uses guidance published by the ICO on their web-site at www.ico.org.uk.

Definition of terms

The following are definitions of the terms used in this document:

The Policy – this Data Protection Policy;

We – SPC;

PD (Personal Data) – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. PD does not include information about organisations, companies and agencies as it applies only to named persons, such as individual volunteers.

Data Subject – the individual, whose PD is being held or processed by SPC, for example a donor or hirer;

Data Controller – SPC, whose Members decide what PD SPC will hold and how it will be stored and processed;

The Legislation – the combined provisions of the DPA and GDPR;

Data Protection Officer (if appointed) – the person responsible for ensuring that SPC follows its Data Protection

Policy and complies with The Legislation *(NB: SPC is not required to appoint a Data Protection Officer)*;

Processing – means collecting, amending, handling, storing or disclosing PD.

Responsibilities

SPC Members, staff and volunteers are personally responsible for processing and using PD in accordance with The Legislation. Those having who have access to PD will therefore be expected to read and comply with this Policy.

SPC is the Data Controller within the terms of The Legislation (ICO registration reference: Z8023511). As such, SPC is legally responsible for complying with The Legislation and determines what purposes any PD held will be used for. SPC will take into account legal requirements, ensure that they are properly implemented, and will through appropriate management and strict application of criteria and controls:

a) Collect and use information fairly;

b) Specify the purposes for which information is used;

c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;

d) Ensure the quality of information used;

e) Ensure the rights of people about whom information is held, can be exercised under The Legislation. These include:

- The right to be informed that processing is undertaken;

- The right of access to one's PD;
- The right to prevent processing in certain circumstances, and;
- The right to correct, rectify, block or erase information which is regarded as wrong information;
- The right to expect that the Data Controller will:
  - Take appropriate technical and organisational security measures to safeguard PD;
  - Ensure that PD is not transferred abroad without suitable safeguards;
  - Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
  - Set out clear procedures for responding to requests for information. All Members, staff and volunteers are aware that a breach of the rules and procedures identified in this Policy may lead to action being taken against them.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to The Legislation. In case of any queries or questions in relation to this Policy, please contact the SPC Parish Clerk.

The Parish Clerk is responsible for:

- Ensuring that SPC complies with the provisions of The Legislation;
- Implementation of this Policy;
- Handling Data Subject access requests in accordance with The Legislation.

SPC and the Parish Clerk may be contacted via the SPC web-site at https://selwoodparishcouncil.gov.uk/

This Policy applies to SPC and its employees. It does not apply to individual Members, except when:

- SPC discloses PD to them so that they can fulfil a SPC function. In such cases those Members are subject to this Policy as if they were employees for as long as the PD remains in their possession.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to The Legislation.

Any queries or questions in relation to this Policy must be addressed to the SPC Parish Clerk.

Data Protection Principles

It is SPC Policy to comply fully with the following Data Protection Principles as defined in The Legislation:

1) PD shall be processed fairly and lawfully and, in particular, shall not be processed unless there is an operational need to do so;
2) PD shall be obtained only for one or more specified and lawful purpose, and shall not be processed in any manner incompatible with that purpose or those purposes;
3) PD shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4) PD shall be accurate and, where necessary, kept up to date;
5) PD processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6) PD shall be processed in accordance with the rights of Data Subjects under The Legislation;
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of PD and against its accidental loss, destruction, or damage;
8) PD shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

Personal Information Processed by SPC

The table below details the kind of PD that is typically in the possession of SPC, the circumstances under which it is acquired, and how it is processed.

General Purpose	Type of Personal Information	Data Handling Policy
As a Parish Council	Member contact details. Additional personal information: photographs for SPC web-site, publications and publicity; DOBs and other personal information to set up Members as signatories for SPC's banking facility.	Held by the Chair of Members and the SPC Parish Clerk. Personal information concerning Members may be published if already in the public domain or with their express consent. Any Member PD relating to SPC's banking facility will be held only for the duration of their term in office.
As an employer	Personal & financial details of employees.	Employee records are held by the Parish Clerk and any Member(s) appointed by minuted decision taken at a full meeting of SPC when required.
Dealings with suppliers	Contact and payment details of the supplier and records relating to supplier performance.	Records are held by the Parish Clerk, and any Member(s) appointed by minuted decision taken at a full meeting of SPC when required.
SPC web-site	The web-site contains only information intended to be made public. It includes a facility for the public to contact the Parish Clerk by email at a SPC address.	This data protection Policy is published on the web-site. The web-site includes appropriate data protection statements.
Parish Surveys / consultation	A respondent may optionally include their name and contact details to enable SPC to verify that the response is valid (from a resident of the Parish) and unique.	Records are held by the Clerk & RFO plus any Member(s) appointed by minuted decision of SPC if required.
Member of the public contacts SPC (as distinct from contacting an individual Member)	Name and contact details in association with the correspondence and possibly information included by the originator.	Contact to SPC is via the Clerk & RFO, Chairman or Vice Chairman. The general issue may be shared with all the Members only after all personal information has been removed, unless the Clerk has express permission from the originator (and any other people cited). Records are held by the Clerk for as long at the issue remains live/unresolved.

Applying The Legislation within SPC

We will let people know why we are collecting their data, which is for the lawful purpose of managing SPC, its hiring, marketing, publicity for events, fundraising and finances. It is our responsibility to ensure PD is only used for this purpose unless specific consent is given or the PD is already in the public domain. Access to PD will be limited to SPC

staff and Members. Where individuals need to be identified in public documents (e.g. minutes) and harm may result, initials rather than full names will normally be used.

Correcting data

Individuals have a right to make a Subject Access Request (SAR) to find out whether SPC holds their PD, where it is held, what it is used for and to have data corrected if it is incorrect. This right exists to prevent use which is causing the Data Subjects damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Before providing any information, the identity of the individual submitting the SAR must be established by means of both photo identification (e.g. passport or photo driving licence) and confirmation of address (e.g. recent utility bill, bank or credit card statement).

Any concerns on the part of Data Subjects about SPC's compliance with a SAR (e.g. if it is manifestly incorrect or excessive) need to be discussed promptly with the Parish Clerk

Procedures for Data Handling & Security

SPC has a duty to ensure that appropriate technical and organisational measures and training are in place to prevent:

- Unauthorised or unlawful processing of PD;
- Unauthorised disclosure of PD;
- Accidental loss of PD.

All Members, staff and volunteers must therefore ensure that PD is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

PD relates to data of living individuals who can be identified from that data and to whom use of that data could cause damage or distress. Mentioning someone's name in a document does not qualify as PD; however, combining various data elements such as a person's name, salary, religious beliefs etc. would be classed as PD, and falls within the scope of The Legislation. It is therefore important that Members, employees and volunteers consider any information (which is not otherwise in the public domain) that can be used to identify an individual as PD and observe the guidance given below.

Privacy Notice and Consent Policy

The privacy notice and consent Policy are as follows:

SPC uses PD for the purposes of managing its affairs and finances, fundraising, running and marketing events, and staff employment. Data may be retained for up to 7 years for accounts purposes and for longer where required, e.g. by SPC's insurers. More detailed information about this is available from the SPC Parish Clerk.

Consent forms, if used, will be stored in a securely-held electronic or paper file.

Operational Guidance

Employees and Members acting on behalf of SPC shall protect personal information within the scope of this Policy in accordance with the following procedures:

Externally-hosted Services (e.g. email, cloud storage services).

External services (e.g. email, cloud storage services) shall be secured with a strong password to prevent access to the account from remote devices.

Email

All Members, staff and volunteers should consider whether an email (whether incoming or outgoing) will need to be kept as an official record. If the email needs to be retained, it should be saved into the appropriate folder or printed and stored securely.

Emails that contain PD no longer required for operational use should be deleted from the personal mailbox and any 'deleted items' box.

Where someone who is not a Member, employee or contractor needs to be copied into an email (e.g. a wider circulation list for an upcoming event), the 'bcc' instead of 'cc' option must be used to avoid their PD being shared through forwarding.

Phone Calls

Phone calls can lead to unauthorised use or disclosure of PD and the following precautions should be taken:

- PD should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for PD to be checked or confirmed, be aware that the caller may be impersonating someone with a right of access.

Personal Computers

Personal computers should be secured with a strong password to prevent unauthorised access to personal information should the aforementioned computer be stolen, passed on or otherwise compromised. Internet-connected devices should be running anti-virus software and be protected by a suitable firewall device such as a properly configured router provided by an Internet Service Provider. Where a personal computer is shared, any personal information subject to this Policy processed on that computer shall be protected by password known only to the employee/Member (for example through the use of a separate user account or password-protected files).

All laptops and portable devices that hold PD must be protected with a suitable password which is changed regularly. Where sensitive data or financial information is held, an encryption program should be used.
Laptops must be locked (password protected) when left unattended, even for short periods of time.

When being transported in a car, laptops must be kept out of sight, preferably in the boot.
Whenever laptops are left in an unattended vehicle, they must be put it in the boot with all doors locked and any alarm set.

Laptops or portable devices must never be left in a vehicle overnight or unattended in restaurants, bars or any other venue.

On public transport, laptops and portable devices must remain in the possession of their keeper at all times and never placed in luggage racks or put down on the floor.

Data Security and Storage

Only the minimum necessary PD should be stored on SPC computers and laptops. PD received on disk or memory stick should be saved to the relevant permanent-storage file. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped.

Passwords

Passwords must not be easy to guess and should contain upper- and lower-case letters and numbers.
Passwords should be 6 characters or more in length. A few common-sense rules for password protection are to:

- never share them with anyone;
- never physically write them anywhere on the protected device or in its case.

Data Storage

PD will be stored securely and will only be accessible to individuals authorised by SPC.
Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. For employee records see below. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when Members, staff or volunteers retire.
All PD held for SPC must be non-recoverable from any computer which has been passed on/sold to a third party.

Personal Mobile Devices & Removable Storage

Employees and Members with mobile devices that are capable of storing personal information and/or sending and receiving email should secure those devices using a PIN or other in-built security facility to prevent unauthorised access to personal information should the device be stolen, passed on or otherwise compromised. USB drives shall not be used.

Taking Information Home

All reasonable steps should be taken to secure electronic and paper-based information whilst in residential property. Information of a sensitive nature, including but not limited to financial documents, cheque books and banking credentials should be kept securely under lock and key.

Information Regarding Employees or Former Employees:

Information regarding an employee or a former employee will be kept indefinitely. This requirement is necessary to enable Members to meet certain obligations such as those relating to employment law, taxation, pensions or insurance.

Visual Images

SPC may use general photographs of groups of adults for publicity purposes in accordance with its lawful basis for using PD. Images of children must not be used without the written consent of their parent or guardian. However, SPC is aware that disclosing the location of children can sometimes put them or their families at risk. Consequently, at large events where publicity photos may be taken, a notice should be posted at the entrance, or an announcement made, providing opportunity for people to opt out of such photographs. At small events, the (verbal) consent of individuals should be obtained if their image will be clearly identifiable.

Data Subject Access Requests

SPC may occasionally need to share PD with other agencies (such as the local authorities, funding bodies and other voluntary agencies) for purposes other than the management or operation of SPC. The circumstances where the law allows SPC to disclose data (including sensitive data) without the Data Subject's consent are:
a) when legally required or as may be authorised by the Parish Clerk of State to vouchsafe the vital interests of a Data Subject or other vulnerable person;
b) when the Data Subject has already made the information public;
c) when required for legal proceedings, obtaining legal advice or defending any legal rights;
d) Monitoring for equal-opportunities purposes – i.e. race, disability or religion.
SPC regards the lawful and correct treatment of PD not only as a pre-requisite for maintaining the confidence of those with whom SPC deals but also as an essential requirement for any organisation to succeed. If an agency asks for PD for any purpose other than mentioned above (e.g. in order to improve a service) a consent form will need to be completed by the Data Subject(s) clearly authorising SPC to pass their PD on.

Disposal of PD

When no longer required, personal information stored electronically shall be deleted from the appropriate applications, including deletion from the 'Recycling Bin' and every reasonable endeavour to remove all copies and backups. (NOTE: Records may persist in electronic backups for long periods. These records are only accessed in exceptional circumstances and any out-of-data personal records shall be deleted at the point they are discovered in backup records.) PD in printed form shall be disposed of in such a way that the information cannot easily be reconstituted, for example by shredding or burning.

Risk Management

The consequences of breaching Data Protection protocols can cause harm or distress to service users through the release of their PD to inappropriate people or the denial of a service to which they are entitled. SPC Members, staff and volunteers should be aware that they can be personally liable if they use PD inappropriately. This Policy is designed to provide clarity, minimise the risks and to ensure that SPC's reputation is not damaged through inappropriate or unauthorised access and sharing.