South Wonston Parish Council
Data Protection Policy

Adopted by South Wonston Parish Council – September 2024

INTRODUCTION

This is the Data Protection Policy of South Wonston Parish Council. Section 7 (3) of the Data Protection Act 2018 (DPA) states that parish councils are not public authorities for the purposes of The General Data Protection Regulations 2018 (GDPR). Parish Councils, nevertheless, are still subject to Data Protection Legislation (DPL) and must have sufficient staff and resources to carry out their obligations under GDPR.

The Parish Council as data controller is entrusted with deciding why and how the data it collects will be processed. It is required under the DPA to gather, hold, process, use, record, store and dispose of all personal information in a secure and confidential manner. Lawful and correct treatment of personal data is crucial for maintaining confidence.

Personal data includes anything that might identify the individual, sometimes referred to as the data subject, or make them identifiable, directly or indirectly by name, any form of identification number, location, postal or online address, factors specific to physical, mental, economic, cultural or social references. Special categories of information include ethnicity, religion, politics, Trade Union membership, genetic, biometric, health, gender, sexuality and criminal offences.

Processing refers to any operation or set of operations performed with automated or manual methods on personal data, including collecting, storing, retrieving, using, combining, erasing or destroying.

This policy applies to all Parish Council employees, councillors, volunteers and contractors. It provides a framework within which the Parish Council will ensure compliance with DPA 2018 and will underpin any procedures and activities connected with the implementation of DPA.

It has been reviewed (2024), revised and updated to reflect changes to data protection legislation (DPL) after the UK's departure from the European Union (EU) 31st January 2020. The GDPR is retained in domestic law as the UK GDPR effective from 1st January 2021, but the UK has the independent ability to keep the framework under review. The UK GDPR accompanies the amended version of the DPA 2018. The key principles, rights and obligations remain the same. Together they constitute

the DPL. On 29th June 2021, the European Commission recognised the UK Data Protection regime as “adequate”, meaning it offers equivalent protection to the EU version. Transfers between the UK, EU and European Economic Area and other compatible data regimes are similarly recognized and may continue as previously.

POLICY STATEMENT

The Parish Council regards the lawful and correct treatment of personal data as essential for maintaining confidence. It will ensure that it treats personal data lawfully and correctly with due regard for the rights and freedoms of individuals and in accordance with the Data Protection Principles set out in Article 5 of the UK GDPR and Sections 35-40 pf the DPA 2018.

ROLES AND RESPONSIBILITIES

A Data Protection Officer (DPO) is generally considered essential for any organisation which handles personal data, including Parish Councils. The role of the DPO is to inform and advise the Parish Council about its data protection obligations, monitor and advise on the processing of personal data and to be the first point of contact with the Information Commissioner’s Office (ICO). They are responsible for the regular review of this policy to ensure the contents are still relevant, efficient and effective.

If the Parish Council can identify a person with appropriate experience and/or training, either an elected member or volunteer, they may be appointed with the approval of the Full Council. Otherwise, the Parish Council will approach the Hampshire Association of Local Councils for support with GDPR processes and DPO services.

The Parish Council is aware that registration as a data controller with the ICO is voluntary.

The Parish Council will ensure that all staff, elected members and volunteers comply with the requirements of this policy and associated policies and procedures. Everyone handling personal data should understand that they are responsible for following good data protection practice and take up training as opportunities arise. All those dealing with enquiries should be fully competent, prompt and polite and understand that they should direct people wishing to complain to the Parish Council’s Complaints Policy and to the ICO for independent advice.

The Parish Council will create contracts which contain mandatory information assurance and make clear to contractors that they are bound by the same code of practice with regard to the DPA as the Parish Council.

The primary role of the Parish Council is to act in accordance with the Data Protection Principles.

Principle 1

Personal information shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Parish Council will observe fully the conditions for lawful gathering and use of individual personal data to make sure processing is fair, legislation-compliant and transparent. The consent of the individual is the most appropriate lawful basis for processing. Obtaining consent is essential for the legitimate conduct of data processing and encourages reputation-enhancing trust and engagement. It gives the individual agency. Explicit consent will be sought before any data operation takes place. The consent giver will be given specific grounds for processing and shown how consent may be withdrawn along with other rights. Other lawful bases for processing to be observed by the Parish Council are a contract with the individual, a legal obligation to comply with the law, vital interests where the individual's life may be in danger, public interests and legitimate interests. The Parish Council will monitor its processing for any unfairness, never obtain data by deceit, handle data correctly and be aware of potential adverse consequences. It will be honest about its use of personal data and always use clear language. The Parish Council will at all times be able to demonstrate compliance with UK GDPR, provision of appropriate policies and processes and accountability for its decisions.

Principle 2

Personal information shall be collected for specific, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

The Parish Council will make very plain all the issues connected with data processing. It will employ a Privacy Notice on its website explaining what kinds of data are collected, how and why, how it will be processed and on what legal basis, how long data is kept and how disposed of, and the obligations of the Parish Council and the rights of individuals who have permitted their data to be used. Any changes to these procedures will only be made with consent or under a clear obligation or legal requirement. Changes will be notified. The Parish Council will comply with obligations to satisfy requests from people wishing to exercise the rights of the individual under DPL to be told whenever processing it being undertaken, to access the information held about them, (see How to Access Your Records) to object to processing, to rectify, restrict or erase their information, to data portability (to ask for personal data to be transferred to another organisation in some circumstances), to be informed of rights in relation to automated decision making and profiting. and the right to withdraw consent already given if a change of mind has occurred.

Principle 3

Personal Information shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The Parish Council will collect and process only as much personal information as it requires for the properly stated purposes for which it is collected. The data will be applicable to those purposes and not held longer than necessary.

Principle 4

Personal information shall be accurate and, where necessary, kept up to date; every reasonably step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

The Parish Council will ensure the information it holds is accurate and up to date. and personal rights to erase or rectify are honoured.

Principle 5

Personal Information shall be kept in a form which permits identification of people for no more than is necessary for the purposes for which the information is processed.

See the Parish Council's Retention and Disposal Policy. Information will not be kept for longer than necessary.

Principle 6

Personal information shall be processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Parish Council will have the utmost regard to the protection of its network and information systems. The security of the Pavilion (doors, locks, alarms, security lighting, CCTV, control of access for visitors, users and computer maintenance experts as required, the disposal of paper and electronic waste and cybersecurity measures for all IT equipment including mobile devices) will be paramount. In addition, risk assessments will be carried out routinely to ensure protection is ongoing.

The Parish Council will ensure appropriate measures are taken to ensure personal information is only processed in a way compatible with DPL to protect personal data against damage, loss or abuse and safeguard individual rights. A GDPR Data Protection Impact Assessment to identify and minimise data processing risks to projects where there may be a high risk to individuals will be carried out as is now mandatory. The ICO will be consulted in case of uncertainty. As a matter of good practice, a DPIA will be undertaken for any new project involving the use of personal data and its principles embedded in any other data processing exercise. The Parish Council will not share personal data with anyone (unless GDPR exemptions apply, such as in the case of law enforcement, tax or health and child considerations, or data sharing agreement) other than specified recipients at the time of collection without obtaining the explicit consent of the owner before sharing to avoid a breach of confidentiality. Data protection breaches will be reported to the ICO and the affected persons as required under DPL. Breaches will also be logged, investigated and measures to prevent re-occurrence applied. The Parish Council will ensure that the disclosure of personal data to third parties in relation to prevention or detection of crime and apprehension or prosecution of an offender is compliant with DPL. It will also comply with DPL if sharing personal information with another data controller by entering into a data sharing agreement where appropriate. The Parish Council will

meet requirements to protect personal data and safeguard individual rights “by default and design”. This will involve measures to ensure only the necessary amount of data is processed only for as long as necessary (default) and addressing compliance with the Data Protection Principles before any new or altered processing is employed (design).

Principle 7

In addition to the six principles above, Article 5 (2) sets out the requirement, referred to as the Accountability Principle, for data controllers to demonstrate that they comply with the Data Protection Principles. This means that the council must keep records of all personal information processing and be able to provide these to the ICO on request.

The Parish Council will keep records of all processing activities which will be made available to the ICO should they be required.

SURVEILLANCE CAMERA SYSTEMS

The Parish Council operates four Closed Circuit Television (CCTV) cameras mounted on the Pavilion. These are regulated by the Surveillance Camera Commissioner’s Personal Information Charter 2021, which is compatible with UK GDPR and the DPA 2018. All operators of surveillance camera systems overtly in public places are encouraged to adopt the provisions of the Surveillance Camera Code of Practice 2022. This gives guidance on the appropriate and effective use of CCTV. South Wonston Parish Council has agreed to abide by this Code of Practice. See Appendix 1 for the Guidance Principles.

ADOPTION OF THIS DOCUMENT

This policy was adopted by South Wonston Parish Council on

It is due for review on

Appendix 1

SURVEILLANCE CAMERA GUIDANCE PRINCIPLES

1 Cameras must be used for a specific purpose in pursuit of a legitimate aim and be necessary to meet an identified pressing need.

2. Operators must take into account the effect on individuals and their privacy which requires reviews to ensure the use remains justified.

3. There must be as much transparency in use as possible, including a published contact point to access to information and the complaints procedure.

4. The operators must demonstrate clear responsibility and accountability for the use of all surveillance camera systems activities including images and information collection held and used.

5. Clear rules, policies and procedures must be in place before the system is used and communicated to all who need to comply with them.

6. No more images and information should be stored than is strictly required for the stated purpose of the surveillance camera system and such images and information should be deleted once the purpose has been discharged.

7. Access to retained images and information should be restricted and clearly defined rules applied to those who can gain access and for what purpose access is granted. The disclosure of images and information should only take place when it is necessary for that purpose or for the purpose of law enforcement.

8. Operators should consider any approved technical and competency standards relative to their system and purpose and work to meet and maintain those standards.

9. Images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. Effective reviews and audit mechanisms to ensure legal requirements, policies and standards should be complied with in practice and regular reports should be published.

11. When used in pursuit of a legitimate aim and pressing need for use, the system should be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evident value.

12. Any information used to support a system which compares against a reference database for matching purposes should be accurate and kept up to date.