

**General Data Protection Regulations**

“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 the General Data Protection Regulation (the “GDPR) and other legislation relating to personal data and rights such as the Human Rights Act. Sidlesham Parish Council (SPC) had therefore adopted a number of policies and procedures to ensure that any data SPC holds is protected. If you feel that a breach has occurred, please contact the Clerk immediately who acts as the Parish Council’s Data Protection Officer.

**Data Subject Access and the Data Protection Act**

Sidlesham Parish Council (SPC) takes your data privacy seriously. If you wish to find out what information SPC holds about you please contact us providing your contact details, a brief description of the information you require and enclose proof of your identity. This could be a scanned copy of a household bill, passport or driving license.

You will receive a response to your request within 20 days.  Please send your request to one of the following:

email address: **parishclerk@sidleshamparishcouncil.gov.uk**

or

by post to:
Sidlesham Parish Council
9 Payne Close
Pagham
West Sussex PO21 4QA

Policies reviewed and updated: September 2024
Annual Review

**Appendix A -** [**Data Protection Registration** **Certificate**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/Registration-Certificate-Z1494803.pdf)

**Appendix B -** [**Data Breach Policy**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-Data-Breach-Policy-July-2024-af.pdf)

**Appendix C -** [**Data Protection Policy**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-Data-Protection-Policy-July-2024.pdf)

**Appendix D -** [**IT, Communications & Monitoring Policy**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-IT-Communications-Monitoring-Policy-July-2024-af.pdf)

**Appendix E –** [**Privacy Statement – General**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-Privacy-Statement-General-July-2024.pdf)

**Appendix F -** [**Privacy Statement – Staff**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-Privacy-Statement-Staff-July-2024.pdf)

**Appendix G -** [**Subject Access Request Procedure**](https://www.wisboroughgreen.org/wp-content/uploads/2024/08/WGPC-Subject-Access-Request-Procedure-July-2024-af.pdf)



**Appendix A**

**Data Protection Registration Certificate**



**Appendix B**

**Data Breach Policy**

**Purpose**

This document defines a Data Breach Incident and the procedure to report an incident.

**Scope**

This document applies to all staff, councillors, volunteers, contractual third parties and agents of SPC who have access to Information Systems or information used for SPC purposes.

**Definition**

An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

An Information Security Incident includes:

• The loss or theft of data or information.

• The transfer of data or information to those who are not entitled to receive that information.

• Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.

• Changes to information or data or system hardware, firmware, or software characteristics without SPC's knowledge, instruction, or consent.

• Unwanted disruption or denial of service to a system.

• The unauthorised use of a system for the processing or storage of data by any person.

**When to report**

All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen. If the breach occurs or is discovered outside of normal working hours, it must be reported as soon as is practicable.

**Action on becoming aware of the incident**

1. The Clerk must be contacted by email or telephone.
2. The Clerk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

• Full and accurate details of the incident.

• When the breach occurred (dates and times).

• Who is reporting it.

• The nature of the personal data information.

• How many individuals are involved.

1. The outcomes of these actions are to be reported to the Clerk who will notify SPC’s designated Data Protection Officer.

**Containment and recovery**

1. The Clerk will first determine if the breach is still occurring. If so, together with the Data Protection Officer and, if appropriate a representative from the IT support company (the Response Team), the appropriate steps will be taken immediately to minimise the effect of the breach.
2. An initial assessment will be made by the Response Team to establish the severity of the breach and whether there is anything that can be done to recover any losses and limit the damage of the breach. That group will also establish who may need to be notified as part of the initial containment and will inform SPC’s Chairman and, where appropriate, the police.

**Investigation and risk assessment**

1. An investigation will be undertaken as soon as reasonably possible, but, generally, within 24 hours of the breach being discovered/reported. The investigation will focus on the cause of the breach, the risks associated with it and will consider:

• the type of personal data involved.

• its sensitivity.

• the protections in place (e.g., encryptions).

• what happened to the data, whether it has been lost or stolen.

• whether the data can be put to any illegal or inappropriate use.

• the affected individuals, and the potential adverse consequences to them (including how serious/substantial these consequences could be, and the likelihood of occurrence).

• whether there are wider consequences to the breach.

• other relevant considerations.

**Notification**

1. The Response Team will determine who needs to be notified of the breach
2. Every incident will be assessed regarding notification on a case-by case-basis, including consideration of the following:

• Are there any legal/contractual notification requirements.

• Will notification assist the individuals affected – can they take actions in relation to the information to mitigate risks.

• Will notification help prevent the unauthorised or unlawful use of personal data.

• Will notification help SPC to meet its obligations under data protection law.

• If many individuals are affected or the consequences are very serious, does the ICO need to be notified.

1. If the Response Team discovers a personal data security breach that poses a risk to the rights and freedoms of individuals, it will report it to the ICO within 72 hours of discovery.
2. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. To the extent feasible, specific, and clear advice will be given on what they can do to protect themselves, including what actions have already been taken to mitigate the risks. Individuals will also be provided with contact details to allow them to contact SPC for further information or to ask questions on what has occurred.
3. The Response Team must also consider notifying third parties such as the police, insurers, banks, or credit card companies, etc. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
4. The Response Team will also consider whether it is appropriate to issue communications to other interested parties.
5. All actions will be recorded by the Clerk.

**Evaluation and response**

1. Once the initial incident is contained, the Response Team will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies or procedures are required.
2. Existing controls will be reviewed to determine their adequacy, and whether any corrective actions should be taken to minimise the risks of similar incidents occurring. The review will consider:

• Where and how personal data is held, stored, and secured.

• Where the biggest risks lie, including any further potential weak points within the existing systems/data protection framework.

• Whether methods of transmission are secure, and compliant with the principle of data minimisation (only sharing the minimum amount of data necessary).

• Identifying weak points within existing security measures. Staff awareness and training.

•Implementing a personal data breach plan and identifying individuals/functions responsible for reacting to reported breaches of security.

1. Any report recommending changes to systems, policies and procedures relating to personal data protection will be considered and approved, as appropriate, by SPC. EXAMPLES OF INFORMATION SECURITY/MISUSE INCIDENT PROTOCOLS Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents. **Malicious Incident**

• Computer infected by a virus or other malware, (for example spyware or adware).

• An unauthorised person changing data.

• Receiving and forwarding chain letters including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.

• Social engineering - unknown people asking for information which could gain them access to SPC data (e.g. a password or details of a third party).

• Unauthorised disclosure of information electronically, in paper form or verbally. • Falsification of records / inappropriate destruction of records.

• Denial of Service, for example - damage or interruption to SPC equipment or services caused deliberately e.g. computer vandalism.

• Connecting non-Council equipment to SPC network.

• Unauthorised information access or use.

• Giving information to someone who should not have access to it - verbally, in writing or electronically.

• Printing or copying confidential information and not storing it correctly or confidentially. **Access Violation**

• Disclosure of logins to unauthorised people.

• Disclosure of passwords to unauthorised people e.g., writing down your password and leaving it on display.

• Accessing systems using someone else's authorisation e.g., someone else's user ID and password.

• Inappropriately sharing security devices such as access tokens.

• Other compromise of user identity e.g., access to network or specific system by unauthorised person.

• Allowing unauthorised physical access to secure premises e.g., server room, scanning facility, dept area.



**Appendix C**

**Data Protection Policy**

**1. Introduction**

1.1. Sidlesham Parish Council (SPC) collects and uses certain types of personal information about staff, councillors, volunteers and other individuals who encounter SPC. SPC may be required by law to collect and use certain types of information to comply with statutory obligations related to employment and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

1.2. GDPR applies to all computerised data and manual files if they come within the definition of a filing system.

**2. Personal Data**

2.1. ‘Personal data’ is information that identifies an individual. A sub-set of personal data is known as ‘personal sensitive data’. This special category data is information that relates to a person’s:

• race or ethnic origin.

• political opinions.

• religious or philosophical beliefs.

• trade union membership.

• physical or mental health.

• an individual’s sex life or sexual orientation.

• genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. SPC does not intend to seek or hold sensitive personal data about staff, councillors, volunteers, allotment holders or other individuals who come into contact with SPC except where it has been notified of the information, or it comes to light via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.

**3. Data Protection Principles**

3.1. Article 5 of the GDPR sets out six data protection principles which must be always followed:

▪ personal data shall be processed fairly, lawfully and in a transparent manner.

▪ Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes.

▪ personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.

▪ personal data shall be accurate and, where necessary, kept up to date.

▪ personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes.

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

3.2. In addition to this:

• SPC is committed to always ensuring that, anyone dealing with personal data shall be mindful of the individual’s rights under the law (as explained in more detail in paragraphs 7 and 8 below).

• SPC is committed to always complying with the principle set out in 3.1. 3.3 This means that we will:

• inform individuals as to the purpose of collecting any information from them, as and when we ask for it and will identify who we will share the information with and how long we intend to retain the information.

• be responsible for checking the quality and accuracy of the information.

• regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy.

• ensure that when information is authorised for disposal it is done in accordance with our disposals policy.

• ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and always follow the relevant security policy requirements.

• share personal information with others only when it is necessary and legally appropriate to do so. • set out clear procedures for responding to requests for access to personal information known as subject access requests.

• report any breaches of the GDPR.

**4. Conditions of Processing**

4.1. The individual has given consent that is specific to the processing activity.

4.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering a contract with the individual, at their request.

4.3. The processing is necessary for the performance of a legal obligation to which we are subject.

4.4. The processing is necessary to protect the vital interests of the individual or another.

**5. Use of Personal Data by the Council**

5.1. SPC collects and uses certain types of personal information about staff, councillors, volunteers, allotment holders and other individuals who encounter SPC. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.

5.2. Any wish to limit or object to use of personal data should be notified to the Clerk in writing. If, in the view of SPC rejection cannot be maintained, the individual will be given written reasons why SPC cannot comply with their request. Staff, Councillors and Volunteers

5.3. The personal data held about staff, councillors, and volunteers may include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs.

5.4. The data is used to comply with legal obligations placed on SPC in relation to employment. We may pass information to other regulatory authorities where appropriate. Personal data will also be used when giving references.

5.5. It should be noted that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period. Other Individuals

5.6. SPC may hold personal information in relation to other individuals who have contact with SPC, such as volunteers and guests.

5.7. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

**6. Security of Personal Data**

6.1. SPC will take reasonable steps to ensure that members of staff, councillors and volunteers will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. SPC will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

**7. Disclosure of Personal Data to Third Parties**

7.1. The following list includes the most usual reasons that SPC will authorise disclosure of personal data to a third party:

• to give a confidential reference relating to a current or former employee;

• for the prevention or detection of crime;

• for the assessment of any tax or duty;

• where it is necessary to exercise a right or obligation conferred or imposed by law upon SPC (other than an obligation imposed by contract);

• for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

• for the purpose of obtaining legal advice.

7.2 SPC may receive requests from third parties to disclose personal data it holds about staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or SPC.

7.3 All requests for the disclosure of personal data must be sent to the Clerk, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

**8. Subject Access Requests**

8.1. Anybody who makes a request to see any personal information held about them by SPC is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

8.2. A subject access request must be made in writing. SPC may ask for any further information reasonably required to locate the information.

8.3. All requests will be handled in line with the Subject Access procedural note.

**9. Other Rights of Individuals Right to Restrict Processing**

9.1. An individual has the right to object to the processing of their personal data and to block or suppress the processing.

9.2. Where such an objection is made, it must be sent to SPC who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

 9.3. SPC shall be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

**Right to Rectification.**

9.4. An individual has the right to request the rectification of inaccurate data or incomplete data without undue delay. Where any request for rectification is received, it should be sent to the Clerk and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified within 20 days.

9.5. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given details of how to appeal to the Information Commissioner.

9.6. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

**Right to Erasure**

9.7. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

• where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.

• where consent is withdrawn and there is no other legal basis for the processing.

• where an objection has been raised under the right to object, and there is no overriding legitimate interest for continuing the processing.

• where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).

• where the data must be erased to comply with a legal obligation.

• SPC will decide regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

**Right to Object**

9.8 An individual has the right to object to:

• ensure that when information is authorised for disposal it is done in accordance with our disposals policy.

• ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and always follow the relevant security policy requirements.

• share personal information with others only when it is necessary and legally appropriate to do so.

• set out clear procedures for responding to requests for access to personal information known as subject access requests.



**Appendix C**

**IT Communications & Monitoring Policy**

**BACKGROUND**

Sidlesham Parish Council (SPC) provides employees and councillors with access to various computer facilities for work and communication purposes. To ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, SPC has adopted an IT, Communications and Monitoring Policy which should be read in conjunction with its Data Protection Policy. SPC makes use of IT systems, for data storage, communications and as a source of information. has adopted an IT, communications, and monitoring policy to:

• prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material);

• protect confidential, personal or commercially sensitive data.

• prevent the introduction of viruses.

• prevent the use of unlicensed software.

• ensure that SPC property is properly looked after; and

• monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

1.SPC provides you with access to various computing, telephone, and postage facilities (“the Facilities”) to allow you to undertake the responsibilities of your position and to improve internal and external communication.

2. This policy sets out SPC’s position on your use of the Facilities and it includes:

• your responsibilities and potential liability when using the Facilities

• the monitoring policies adopted by SPC; and

• guidance on how to use the Facilities.

3. This policy has been created to:

• ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring

• protect SPC from the risk of financial loss, loss of reputation or libel; and

• ensure that the Facilities are not used to cause harm or damage to any person or organisation.

4. This policy applies to the use of:

• local, interoffice, national, and international, private or public networks and all systems and services accessed through those networks.

• desktop, portable and mobile computers, and applications.

• social media; and

• electronic mail and messaging services. COMPUTER FACILITIES: USE OF COMPUTER SYSTEMS

5. Subject to anything to the contrary in this policy, the Facilities must be used for SPC business purposes only.

6. To maintain the confidentiality of information held on or transferred via SPC's Facilities, security measures are in place and must be always followed. A log-on ID and password is required for access to the SPC’s network. This will be changed regularly and must be kept secure and not shared with anyone.

7. You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of SPC or its clients other than in the normal and proper course of carrying out your duties for SPC.

8. To ensure proper use of SPC’s computers, you must adhere to the following practices:

• anti-virus software must be kept always running.

• media storage such as USB drives, CD’s or portable hard drives will not be permitted unless they have been provided by the IT supplier.

• obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers).

• all files must be stored on the network drive which is backed up regularly to avoid loss of information; and

• always log off the network before leaving your computer for long periods of time or overnight.

**SOFTWARE**

9. Software piracy could expose both SPC and the user to allegations of intellectual property infringement. SPC is committed to following the terms of all software licences to which SPC is a contracting party. This means that:

• software must not be installed onto any of SPC’s computers unless this has been approved in advance by our IT Contractors. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities; and

• software should not be removed from any computer, nor should it be copied or loaded on to any computer without prior consent. LAPTOP COMPUTERS, PC’S, TABLETS AND SMARTPHONES

10. Laptop computers, PC’s, tablets, and smartphones belonging to SPC along with related equipment and software are subject to all SPC's policies and guidelines governing non-portable computers and software. All laptops, PC’s and tablets will be encrypted. When using such equipment:

• you are responsible for all equipment and software until you return it. It must be always kept secure.

• you are the only person authorised to use the equipment and software issued to you. • if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to SPC's attention.

• upon the request of SPC at any time, for any reason, you will immediately return any equipment and all software to SPC; and

• if you are using your own laptop or PC to connect with SPC’s network or to transfer data between the laptop or PC and any of SPC's computers you must ensure that you have obtained prior consent, comply with instructions, and ensure that any data downloaded or uploaded is free from viruses. EMAIL (INTERNAL OR EXTERNAL USE)

11. All staff and councillors will be issued in due course SPC email account which must be used when transacting on behalf of SPC.

12. Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. Do not send attachments containing personal data, always use a password protected email. 13. Email should be treated as any other documentation. If you would normally retain a certain document in hard copy, you should retain the email.

14. Do not forward email messages unless the original sender is aware that the message may be forwarded or identifying information has been redacted. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

15. Your email inbox should be checked on a regular basis.

16. As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

17. Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

18. Staff and councillors will be required to surrender their email account and all its contents to SPC if they decide to leave the Council.

**INTERNET**

19. Posting information on the internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. The Clerk is authorised to post on SPC’s behalf.

20. Using the internet for the purpose of trading or carrying out any business activity other than SPC business is strictly prohibited, apart from activities approved by SPC.

21. For the avoidance of doubt the matters set out above include use of wireless facilities.

**MONITORING POLICY**

22. The policy of SPC is that we may monitor your use of the Facilities.

23. SPC recognises the importance of an individual’s privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities. SPC may from time to time monitor the Facilities. Principal reasons for this are to:

• detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.

• ensure compliance of this policy.

• detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of SPC.

• ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time; and

• monitor and protect the wellbeing of employees.

25. SPC may adopt at any time several methods to monitor use of the Facilities. These may include:

• recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.

• recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited.

• physical inspections of individual users’ computers, software and telephone messaging services.

• periodic monitoring of the Facilities through third party software including real time inspections.

• physical inspection of an individual’s post; and

• archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

26. SPC will not (unless required by law):

• allow third parties to monitor the Facilities (except for our appointed IT supplier); or

• disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.

27. SPC may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

**SOCIAL MEDIA**

28. SPC may use social media to communicate messages and will only be used:

• by the CEO, trustee board and persons nominated by them.

• to transmit factual information and news, not personal opinion.

• to respond to comments and requests submitted via the account.

29. Staff using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of SPC.

**GENERAL GUIDANCE**

30. Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

31. When using email or sending any form of written correspondence:

• be careful what you write, never forget that email and written correspondence are not the same as conversation: they are a written record and can be duplicated at will.

• use normal capitalisation and punctuation; typing a message all in capital letters is the equivalent of shouting at the reader.

• check your grammar and spelling; and

• do not forget that emails and other forms of correspondence should maintain the high standards expected by SPC.

**BREACH OF THE POLICY**

32. Observation of this policy is mandatory and forms part of the terms and conditions of employment of staff and Code of Conduct for councillors.

33. Breach of this policy will be regarded as a disciplinary offence and will be dealt with under SPC's formal employee disciplinary process. For councillors, the local monitoring officer would be contacted.

34. Anyone who considers that there has been a breach of this policy in relation to personal information about them held by SPC should raise the matter via SPC's formal grievance procedure



**Appendix E**

**Privacy Statement General**

**Your personal data – what is it?**

“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 (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

**Who are we?**

This Privacy Statement is provided to you by Sidlesham Parish Council (SPC) which is the data controller for your data. Other data controllers SPC works with:

• Local authorities

• Community groups

• Charities

• Other not for profit entities

• Contractors

• Credit reference agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to SPC. If we and the other data controllers listed above are processing your data jointly for the same purposes, then SPC and the other data controllers may be “joint data controllers” which mean we are all collectively responsible to you for your data.

Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller. A description of what personal data SPC processes and for what purposes is set out in this Privacy Notice.

SPC will process some or all of the following personal data where necessary to perform its tasks:

• Names, titles, and aliases, photographs.

• Contact details such as telephone numbers, addresses, and email addresses.

• Where they are relevant to the services provided by SPC, or where you provide them to us, we 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 Hall or room, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

• The personal data we process 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. How we use sensitive personal data: SPC may process sensitive personal data including, as appropriate:

• Information about your physical or mental health or condition to monitor sick leave and take decisions on your fitness for work.

• Your racial or ethnic origin or religious or similar information to monitor compliance with equal opportunities legislation.

• To comply with legal requirements and obligations to third parties.

• These types of data are described in the GDPR as “Special categories of data” and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.

• We may process special categories of personal data in the following circumstances:

 • In limited circumstances, with your explicit written consent.

• Where we need to carry out our legal obligations.

• Where it is needed in the public interest.

• Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

**Do we need your consent to process your sensitive personal data?**

In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

SPC will comply with data protection law. This says that the personal data we hold about you must be:

• Used lawfully, fairly and in a transparent way.

• Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

• Relevant to the purposes we have told you about and limited only to those purposes.

 • Accurate and kept up to date.

• Kept only as long as necessary for the purposes we have told you about.

• Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

SPC uses your personal data for some or all of the following purposes:

• To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services.

• To confirm your identity to provide some services.

• To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp).

• To help us to build up a picture of how we are performing.

• To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions.

• To enable us 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 SPC.

• To maintain our own accounts and records.

• To seek your views, opinions or comments.

• To notify you of changes to our facilities, services, events and staff, Councillors and other role holders.

• To send you 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 SPC.

• To allow the statistical analysis of data so we can plan the provision of services.

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

**What is the legal basis for processing your personal data?**

SPC is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of SPC’s statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using SPC’s services. We will always consider your interests and rights.

This Privacy Notice sets out your rights and SPC’s obligations to you. We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter a contract. An example of this would be processing your data in connection with the use of hall rental facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

**Sharing your personal data**

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

• The data controllers listed above under the heading “Other data controllers SPC works with”.

• Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software.

• On occasion, other local authorities or nonprofit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

**How long do we keep your personal data?**

We will keep some records permanently if we are legally required to do so. We may keep other records for an extended period. For example, it is currently best practice to keep financial records for a minimum period of 7 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority.

SPC 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). We will retain some personal data for this purpose if we believe it is necessary to be able to defend or pursue a claim.

In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

**Your rights and your personal data**

You have the following rights with respect to your personal data. When exercising any of the rights listed below, to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

**The right to access personal data we hold on you**

At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we 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.

**The right to correct and update the personal data we hold on you**

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

**The right to have your personal data erased**

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold. When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

**The right to object to processing of your personal data or to restrict it to certain purposes only**

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.



**Appendix F**

**Privacy Statement – Staff**

**WHO WE ARE**

For the purposes of Data Protection legislation, Sidlesham Parish Council (SPC) is the Data Controller. This means it oversees personal data about you.

 The postal address of the Council is: 9 Payne Close, Pagham, West Sussex PO21 4QA

The Data Protection Officer for the Council is Alison Colban. She can be contacted at:

9 Payne Close, Pagham, West Sussex PO21 4QA

Telephone: 07386731159

Email: parishclerk@sidleshamparishcouncil.gov.uk

In this policy ‘we’ and ‘us’ means SPC.

**HOW WE USE YOUR INFORMATION**

We process personal data relating to those we employ to work at, or otherwise engage to work at, SPC. This is for employment purposes to assist in the running of SPC and/or to enable individuals to be paid.

This personal data includes identifiers such as names and national insurance numbers, employment contracts and remuneration details, qualifications and absence information. It will also include sensitive personal data such as ethnic group, medical information and trade union membership (if you choose to supply this information to us).

During the recruitment process we may receive information about you from a previous employer which you have previously attended. You will know about this because you will have supplied us with the relevant contact details. Collecting and using your information in this way is lawful because:

• The processing is necessary for the performance of your employment contract.

• The processing is necessary for the performance of a legal obligation to which SPC is subject.

• The processing is necessary for the performance of our function, which is a function in the public interest.

When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you to provide it, and whether there is a legal requirement on SPC to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

**HOW WE SHARE YOUR INFORMATION WITH THIRD PARTIES**

We will not share information about you with third parties without your consent unless the law allows us to. We disclose details about you including national insurance number and absence information to our payroll provider to enable you to be paid. We share your details with your pension provider to make sure that you pay the correct amount and maintain your entitlement to a pension upon your retirement. Our disclosures to third parties are lawful because one of the following reasons applies:

• The disclosure is necessary for the performance of your employment contract.

• The disclosure is necessary for the performance of our function which is a function in the public interest.

**HOW LONG WE KEEP YOUR PERSONAL INFORMATION**

We only keep your information for as long as we need it or for as long as we are required by law to keep it. Full details are given in our records retention policy available on www.sidleshamparishcouncil.gov.uk

**YOUR RIGHTS**

You have the right to:

• Ask for access to your personal information.

• Ask for rectification of the information we hold about you.

• Ask for the erasure of information about you.

• Ask for our processing of your personal information to be restricted.

• Data portability.

• Object to us processing your information.

If you want to use your rights, for example, by requesting a copy of the information which we hold about you, please contact the Parish Council Clerk. More information about your rights is available in our Data Protection Policy available on [www.sidleshamparishcouncil.gov.uk](http://www.sidleshamparishcouncil.gov.uk).

If at any time you are not happy with how we are processing your personal information then you may raise the issue with the Data Protection Officer and if you are not happy with the outcome you may raise a complaint with the Information Commissioner’s Office: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Telephone Number: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.



**Appendix G**

**Subject Access Request Procedure**

**HOW TO DEAL WITH A REQUEST FOR INFORMATION: A STEP-BY-STEP GUIDE**

**What is a subject access request (SAR)?**

By law, people can ask you for a copy of any information that has to do with them. It might be saved on your system, but if it’s about them, it’s their personal data, and they have a right to see it. If they ask you for a copy of it, by phone, in person, or in writing, they have made a ‘subject access request’, and you need to act.

**STEP ONE**: Choose a Data Protection lead. The Parish Council Clerk will act as the Data Protection Lead.

**STEP TWO**: Know who is making the request If you’re not sure the requester is who they say they are, you must check this quickly. You can ask questions that only they would know about reference numbers or appointment details for example. Or you can ask for ID that you can verify. There’s little point insisting on photo ID if you don’t know what the requester looks like – it should be proportionate.

**STEP THREE**: Check authorisation If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), check they are allowed to receive it. You will need to see that they have written authority to act on behalf of the person concerned, or a document showing general power of attorney. In most cases, children over 12 can make their own SARs. If you are asked for personal data about a 12-year-old by their parent or carer, you should usually get permission from the child first.

**STEP FOUR**: Set yourself some reminders You have one calendar month to get what you need together and send it to the relevant person. If you need to check their ID or ask for other information, you can wait until they reply before starting the clock on the one-month time limit. However, you should ask for any additional information you need as soon as possible. There are three important things to know about the one calendar month time frame:

1. It does not matter if the day you receive the request is not a working day. For example, if you receive a request on Saturday 7 March, you should respond by Tuesday 7 April.

2. If the SAR’s due date falls on a weekend or a public holiday, you have until the next working day to respond. For example, if you receive a request on 25 November, you should respond by 27 December.

3. You can’t add extra days when the calendar month is shorter. For example, if you receive a request on the 31 January, you should respond by the 28 February. If it is a very complex request, or if the requester has made a lot of requests, you can take an extra two calendar months to respond. But you must let the requester know there will be a delay before the end of the first calendar month.

**STEP FIVE**: Check you are on the same page about what they’ve asked to see If you have the request in writing, read it carefully. It would be easy to assume they are asking for everything you retain when in fact they have only asked for data relating to one subject. They might even be able to give you advice on how to find it. It is okay to ask them. It could save you both some time.

**STEP SIX**: Search for the relevant information Use the search functions on your smartphone, computer (including archived files), and email folders to find information relating to the person, just as you would normally do when looking for a particular file.

You might need to think creatively about all the places where this information might be held. If you are using Office 365 there is a facility to search for information which your IT support can help you to do. You might need to check external hard drives, tablets, portable memory sticks, voice recordings, social media posts and CCTV files, too. Keep looking until you are satisfied there is nowhere else to look.

**STEP SEVEN**: Check what you need to redact before you consider giving the requester their information, look through it carefully to make sure it really is their information. For example, if you have an email that mentions several different people, you should ‘redact’ (black out) any information which does not relate to the person making the SAR. This is important, because most of the time you should avoid disclosing information about other people.

Another way of doing this is to copy and paste sections relevant to the SAR into a separate document and send them that instead. If you are using a computer to redact information, make sure you get advice on how to save it as a new file. Otherwise, there is a risk that someone could delete your blacked-out sections and read the text underneath.

**STEP EIGHT**: Consider the impact of releasing data about other people. Most of the time, you should avoid disclosing information about other people in a SAR, but there may be occasions when the personal data you have pulled together includes information that is closely linked to someone else. In those situations, your aim should still be to release the personal data requested. However, you also need to consider that in doing so you may disclose data about someone else and, at the same time, consider the impact of that.

**STEP NINE**: Prepare your reply If you received the SAR by email, you should reply by email, unless the requester has said otherwise. Check with them what format they would like it sent in and give it a final check with steps seven and eight in mind.

**STEP TEN**: Send your reply securely and keep a record of what you have sent. As well as the requester’s personal data, you need to send your privacy information. They have a right to know why you hold their data, how you got it, how long you are planning on keeping it, who you share it with, and how they can ask for it to be changed (such as updating their address) or deleted. Make sure you keep dated records of the information you send as you may need to refer to it again, for example if they are unhappy with your response or make another request soon after.