

## SEVERN STOKE AND CROOME D'ABITOT PARISH COUNCIL – WORCESTERSHIRE

### DATA PROTECTION POLICY, INFORMATION SECURITY & PRIVACY NOTICE

#### FULL VERSION

---

Published by WCALC: N/A.

Adopted by this Parish Council 11<sup>th</sup> March 2020.

Reviewed Feb 2024.

We are a grouped parish council, comprised of the two Parish Areas of Severn Stoke and of Croome d'Abitot

Contact details Parish Clerk, Lisa Stevens, 07950256363 severnstokeandcda@gmail.com

[A shortened version of our Privacy Notice is available \(summary document\)](#)

#### 1. Introduction

1.1 **Who are we?** This Privacy Notice is provided to you by Severn Stoke and Croome d'Abitot Parish Council which is the data controller for your data in this instance. There are other data controllers, depending on the topic and circumstances.

1.2 This Parish Council needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. We hold and process personal data about our employees, councillors, customers, residents, suppliers and other individuals for a variety of Council purposes, including administrative, legal and commercial purposes.

1.3 This personal information must be collected and dealt with appropriately whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998 AND the 2018 General Data Protection Regulations (GDPR). This policy sets out how we seek to protect personal data, including who can have access to it. It also ensures that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

#### 2. Information Security Responsibilities

2.1 The Council believes that information security is the responsibility of all members of staff. Every person handling information or using Council information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.

2.2 This Policy is the responsibility of Severn Stoke and Croome d'Abitot Parish Council; supervision of the Policy will be undertaken by the Clerk. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Clerk and other designated personnel with security responsibilities in specified areas of the Council.

### 3. Your personal data

3.1 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 (GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

3.2 You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer (or, in this case the Parish Clerk) so that they can update your records.

Contact Parish Clerk [severnstokeandcda@gmail.com](mailto:severnstokeandcda@gmail.com)

07950256363

#### **4. Common terms:**

**Data Controller** – The person who (either alone or with others) decides what personal information this Parish Council will hold and how it will be held or used.

**Data Protection Act 1998** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**The Data Protection Bill (new version)** will (amongst other things):1) Ensure data protection rules are suitable for the digital age. 2) Empower individuals to have more rights/control over their personal data. 3) Give people the right to be forgotten

**Data Protection Officer** – The person(s) responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998 and GDPR.

**Data Subject/Service User** – The individual whose personal information is being held or processed by this Parish Council (for example: a client, an employee, a supporter)

**Explicit consent** – is a freely given, specific and informed agreement by a Data Subject to the processing\* of personal information\* about her/him. Explicit consent is needed for processing sensitive\* data \* See definition

**General Data Protection Regulations (GDPR)** - The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU.

**Notification** – Notifying the Information Commissioner about the data processing activities of this Parish Council, as certain activities may be exempt from notification.

**Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998 and GDPR.

**Processing** – Means collecting, amending, handling, storing or disclosing personal information

**Personal Information/Data** – Information about individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons. Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents,

market traders, hirers, correspondents. Personal data we gather may include: individuals contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records

**Sensitive data** – means data about: • Racial or ethnic origin, • Political opinions, • Religious or similar beliefs, • Trade union membership • Physical or mental health, • Sexual life, • Criminal records, • Criminal proceedings.

**Business Purposes** - The purposes for which personal data may be used by this Parish Council: Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes. Council purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations or in connection with legal proceedings or requests
- Ensuring Council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, recording transactions, training/quality control, security vetting and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff.
- Promoting Council services / Improving Council services

## **5. Data Controller**

5.1. Severn Stoke and Croome d’Abitot Parish Council is the Data Controller, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

## **6. Data Protection Officer (DPO)**

**6.1 Section 7(3) of the DPA says that parish councils are not public authorities for the purposes of GDPR and therefore it is not mandatory to appoint a DPO.** In this instance all queries should be referred to the parish clerk.

6.2 The role of a DPO includes:

- a. Inform and advise about obligations to comply with GDPR and the Data Protection Bill
- b. Monitor compliance and manage internal data protection activities
- c. Be first point of contact for supervisory authorities and for individuals whose data is processed.
- d. A DPO is not personally responsible and data protection compliance remains the responsibility of the data controller and/or data processor.
- e. Keeping the Council updated about data protection responsibilities, risks and issues
- f. Reviewing all data protection procedures and policies on a regular basis.
- g. Assisting with data protection training and advice for all staff members and those included in this policy.
- h. Answering questions on data protection from staff, council members and other stakeholders.
- i. Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by this Parish Council.
- j. Checking and approving with third parties that handle the council’s data any contracts or agreement regarding data processing

#### **h. Supplementary responsibilities of the Parish Councillors (Members):**

- i. They represent residents of their ward, for example, in dealing with questions/requests/complaints;
- ii. They act as a member of the council, for example, as a cabinet member or member of a committee; and
- iii. They may represent a political party, particularly at election time.
- iv. Approving data protection statements attached to emails and other marketing copy.
- v. Addressing data protection queries from clients, target audiences or media outlets.
- vi. Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.
- vii. Reporting breaches - All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Parish Council to:
  - Investigate the failure and take remedial steps if necessary
  - Maintain a register of compliance failures
  - Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

#### **7. Disclosure to Parish Councillors**

7.1 Local authorities can disclose personal information to a councillor if they need to access and use the information to carry out official duties. For this purpose, councillors are in the same position as an employee.

7.2 A local authority (parish council) does not generally have to get the express consent of an individual to disclose their personal information to an elected member of this parish council, as long as:

- the elected member represents the ward in which the individual lives;
- the elected member makes it clear that they are representing the individual in any request for their personal information to the local authority; and
- the information is necessary to respond to the individual's communication.

7.3 In these circumstances, the individual has provided implied consent to the processing of their personal data that is reasonably necessary to pursue the communication/complaint/request/enquiry/action.

7.4 There may be occasions when it is advisable to get an individual's signed consent. However, in most cases, the individual would reasonably expect their sensitive personal data to be disclosed in order to respond to their communication etc. The Data Protection (Processing of Sensitive Personal Data) (elected Representatives) Order 2002 No. 2905 covers this, as it provides a basis for:

- the processing of sensitive personal data by elected representatives in connection with their function as a representative, including the disclosure of such information where necessary; and
- the disclosure of sensitive personal data by organisations responding to elected representatives acting on behalf of individual constituents.

7.5 When providing personal information to the elected member, the local authority should make clear that it is provided only to help the individual and must not be used for any other purpose. Local authorities may wish to do this for each disclosure or more generally lay down a code of practice for councillors to follow. It is good practice to keep a record of any requests by elected members for personal information.

7.6 Where the councillor is able to take a copy of the personal information away or where they have remote access to the information, this parish council specifies that in order to keep the information secure, information must be stored on a password protected computer/laptop. Care must be taken to avoid printing personal information on to paper – where this becomes necessary, care must be taken to ensure it is stored securely and no other person outside the council has access to it.

7.7 The above section 7 taken from “*Disclosure of personal information by local authorities to councillors. Data Protection Act. ICO publication, v 3.0*”

## **8. Disclosure to other agencies**

8.1 Severn Stoke and Croome d’Abitot Parish Council may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The Data Subject will be made aware in most circumstances how and with whom their information will be shared.

8.2 There are circumstances where the law allows this Parish Council to disclose data (including sensitive data) without the data subject’s consent, to:

- Other local authorities;
- Community groups;
- Charities;
- Other not for profit entities;
- Contractors;

8.3 We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be “joint data controllers” which means 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 the council processes and for what purposes is set out in this Privacy Notice.

8.4 These circumstances of legal disclosure are:

- A. Carrying out a legal duty or as authorised by the Secretary of State
- B. Protecting vital interests of a Data Subject or other person
- C. The Data Subject has already made the information public
- D. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- E. Monitoring for equal opportunities purposes – i.e. race, disability or religion
- F. Providing a confidential service where the Data Subject’s consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.
- G. Covered by section above ‘Disclosure to Parish Councillors’. Section 7 above.

8.5 The council 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 the council, 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, financial identifiers, bank account numbers, payment card nos, payment/transaction id, policy numbers, 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.

**9. We use 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 the council;
- 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 the council;

**10. Lawful treatment**

10.1 Severn Stoke and Croome d’Abitot Parish Council regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

10.2 To this end, this Parish Council will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998 (to be replaced shortly by a new Data Protection Bill currently going through the House of lords) AND in the General Date Protection Regulations (GDPR).

**10.3 Specifically, that personal information/PERSONAL DATA is:**

- a) processed lawfully, fairly and in a transparent manner in relation to individuals, and, in particular, shall not be processed unless specific conditions are met;

- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ie. You must have a valid lawful basis in order to process personal data. You must determine your lawful basis before you begin processing, and you should document it.
- c) Necessary to deliver our services.
- d) In the legitimate interests of the Parish Council, parish and parishoners and not unduly prejudice the individual's privacy. In most cases this provision will apply to routine business processing activities.
- e) adequate, relevant and not excessive in relation to the purposes for processing;
- f) Shall be accurate and, where necessary, kept up to date,
- g) 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
- h) processed in a manner that ensures appropriate security of the personal data and shall be processed in accordance with the rights of data subjects under the Act,
- i) the controller shall be responsible for/able to demonstrate, compliance with the principles. (Article 5(2))
- j) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- k) 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 information.
- l) A privacy notice should include the lawful basis for processing as well as the purposes of the processing.
- m) **Sensitive personal data** - In most cases where this Parish Council processes sensitive personal data we (GPC) will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we (GPC) are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.
- n) **Further information on How we use sensitive personal data**
  - We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order 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.

## **11 GDPR - What are the lawful bases for processing?**

11.1 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever this Parish Council processes personal data:

- a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. This includes ‘Disclosure to Parish Councillors’ as described above.
- b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- c) **Legal obligation:** processing is necessary for you 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 you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. This includes ‘Disclosure to Parish Councillors’ as described above.

11.2 The lawful basis for processing can also affect which rights are available to individuals.

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	X but right to withdraw consent
Contract	✓	✓	X
Legal obligation	X	X	X
Vital interests	✓	X	X
Public task	X	X	✓
Legitimate interests	✓	X	✓

## 12 Criteria and controls

12.1 Severn Stoke and Croome d’Abitot Parish Council will, through appropriate management, apply criteria and controls:

- a) Observe fully, conditions regarding the fair collection and use of information,
- b) Meet its legal obligations to specify the purposes for which information is used,
- c) Collect and process appropriate information, 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 that the rights of people about whom information is held, can be fully exercised,

12.2 These include:

- a) The right to be informed that processing is being undertaken,
- b) The right of access to one’s personal information
- c) The right to prevent processing in certain circumstances and
- d) The right to correct, rectify, block or erase information which is regarded as wrong information
- e) The right to be forgotten\*.
- f) Take appropriate technical and organisational security measures to safeguard personal information,
- g) Ensure that personal information is not transferred abroad without suitable safeguards,
- h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- i) Set out clear procedures for responding to requests for information.



### **\* More on the right to be forgotten**

12.3 A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

### **13. Data collection - Informed consent**

13.1 Informed consent is when:

- a) A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- b) and then gives their consent.

13.2 IMPORTANT: The scenario/s where specific consent will not be sought is described above in the section 'Disclosure to Parish Councillors'. (7 above)

### **14. Information provided to Data subject**

14.1 Severn Stoke and Croome d'Abitot Parish Council will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

14.2 When collecting data, unless covered in the section 'Disclosure to Parish Councillors above, the Parish Council will ensure that the Data Subject:

- a) Clearly understands why the information is needed
- b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- c) As far as reasonably possible and excepting the scenario/s described in the section above (Disclosure to Parish Councillors), grants explicit consent, either written or verbal for data to be processed
- d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- e) Has received sufficient information on why their data is needed and how it will be used
- f) Has received information about how to make enquires and how/who should be contacted in order to access personal information or to exercise the right to be forgotten.
- g) Our Privacy Notice details further on data protection. The notice:
  - Sets out the purposes for which we hold personal data on customers, employees, residents and service users.
  - Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers.
  - Provides that service users and correspondents have a right of access to the personal data that we hold about them

### **15. Internal Staffing Records**

15.1 Internal staffing records that should be kept by the council but which still fall under GDPR, include:

- a) personal employee details such as name and address/ next of kin/ banking details/ National Insurance information
- b) the employee's employment history with the council
- c) a copy of the employee's contract of employment
- d) holiday records
- e) absence records including sickness absence

- f) details of any disciplinary action taken against the employee or grievances brought by the employee
- g) the original job application information with details of previous employment history, qualifications and references obtained.

## **16. Data Storage and Information Security**

16.1 Severn Stoke and Croome d’Abitot Parish Council recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the Council will facilitate the secure and uninterrupted flow of information, both within the Council and in external communications.

16.2 The Council believes that security is an integral part of the information sharing which is essential to corporate endeavour and the policies outlined below are intended to support information security measures throughout the Council. This policy is based on recommendations contained in British Standard 7799 – A Code of Practice for Information Security Management.

16.3 Definition of information security . For the purposes of this document, information security is defined as the preservation of: • confidentiality: protecting information from unauthorised access and disclosure; • integrity: safeguarding the accuracy and completeness of information and processing methods; and • availability: ensuring that information and associated services are available to authorised users when required.

16.4 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

16.5 Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

16.6 Information will be stored for only as long as it is needed/necessary or required statute and will be disposed of appropriately. It is this Parish Council responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

16.7 What is ‘necessary’ will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

16.8 More on storing data securely:

- a) In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- b) Printed data should be shredded when it is no longer needed. It is acceptable to commission a third party organisation to shred such documentation. In this instance, this parish council uses ‘Storage king, Worcester’ for this operation.
- c) Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- d) Data stored on CDs or memory sticks must be locked away securely when they are not being used
- e) The DPO must approve any cloud used to store data
- f) Servers containing personal data must be kept in a secure location, away from general office space

- g) Data should be regularly backed up in line with the council's backup procedures
- h) Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- i) All servers containing sensitive data must be approved and protected by security software and strong firewall.

## **17. Compliance with Legal and Contractual Requirements**

**17.1 Authorised Use** Council facilities must only be used for authorised purposes. The Council may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

**17.2 Access to Council Records** In general, the privacy of users' files will be respected but the Council reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with Council policies and regulations, and to determine which records are essential for the Council to function administratively. Except in emergency circumstances, authorisation for access must be obtained from the Clerk, or nominee, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

**17.3 Protection of Software** To ensure that all software and licensed products used within the Council comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, the Council will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

**17.4 Virus Control** The Council will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of Council computers, including laptops, shall comply with best practice, in order to ensure that up-to-date virus protection is maintained on their machines.

## **18. Retention and Disposal of Information**

**18.1** All staff have a responsibility to consider security when disposing of information in the course of their work. Retention periods for some kinds of personal information are listed in the Parish Council Policy advising of Document Retention Guidelines.

## **19. Data access and accuracy**

**19.1** All Data Subjects have the right to access the information this Parish Council holds about them. Severn Stoke and Croome d'Abitot Parish Council will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

**19.2** Data portability - Upon request, a data subject has the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

**19.3** In addition, this Parish Council will ensure that:

- a) It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection. Parish Councils have been provided with a waiver for the need to appoint a Data Protection Officer. In this case this Parish Council is currently investigating the appointment of its Parish Clerk to fulfil this function.

- b) Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- c) Everyone processing personal information is appropriately trained to do so,
- d) Everyone processing personal information is appropriately supervised,
- e) Anybody wanting to make enquiries about handling personal information knows what to do,
- f) It deals promptly and courteously with any enquiries about handling personal information,
- g) It describes clearly how it handles personal information,
- h) It will regularly review and audit the ways it holds, manages and use personal information
- i) It regularly assesses and evaluates its methods and performance in relation to handling personal information
- j) All staff, Cllrs and Lengthsman (past and present) are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

#### 19.4 More on Accuracy and relevance:

- k) We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
- l) Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Mrs Lisa Stevens.

## 20. Reporting

20.1 All staff and other users should report immediately to the Clerk, • any observed or suspected security incidents where a breach of the Council's security policies has occurred, • any security weaknesses in, or threats to, systems or services. 8.2 Software malfunctions should be reported to the Clerk.

### Footnote:

Clerk & RFO Mrs Lisa Stevens, 9 The Limes, Kempsey, Worcs, WR5 3LG. Tel: 01905 820956 Mob: 07950256363. Email: [severnstokeandcda@gmail.com](mailto:severnstokeandcda@gmail.com). <http://e-services.worcestershire.gov.uk/MyParish>

Requests for this information in other languages/audio/large print will be reasonably considered.