WATCHFIELD PARISH COUNCIL

DATA PROTECTION POLICY

Watchfield Parish Council (WPC) is committed to compliance with the requirements of the Data Protection Act 1998 which came into effect on 1 March 2000 and the General Data Protection Regulations 2018. WPC will, therefore, follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Data Protection Act.

The policy uses guidance published by the Information Commissioner's Office (ICO) ico.org.uk

The Clerk to the Council is responsible for:
• Ensuring that the Parish Council complies with the provisions of the DPA;
• Implementation of this policy;
• Handling subject access requests in accordance with the DPA.

The Parish Council and Clerk may be contacted via the Parish Council web site: www.watchfield.org

Statement of policy
In order to operate efficiently, WPC has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirement of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used.

It should be understood that all information given at a public meeting of WPC is in the public domain, is likely to appear in minutes and may be reported by the press.

THE GENERAL DATA PROTECTION REGULATION: The General Data Protection Regulation 2018 says that the information provided to people about how we process their personal data must be concise, transparent, intelligible and easily accessible, written in clear and plain language, particularly if addressed to a child and free of charge.

As a local authority WPC has a number of procedures in place to ensure that it complies with The Data Protection Act 1998 and the General Data Protection Regulation 2018 when holding personal information. WPC has appointed the Clerk as the designated Data Protection Officer. The clerk and council will receive training for this role, as required.

When dealing with personal data, WPC staff and Councillors must ensure that: -

- IT IS PROCESSED FAIRLY AND LAWFULLY. This means that information should only be collected from individuals if staff and Councillors have been open and honest about why they want the information.
- IT IS PROCESSED FOR SPECIFIED PURPOSES ONLY
- IT IS RELEVANT TO WHAT IT IS NEEDED FOR. Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
- IT IS ACCURATE AND KEPT UP TO DATE. Personal data should be accurate, if it is not it should be corrected.
- IT IS NOT KEPT LONGER THAN IT IS NEEDED
- IT IS PROCESSED IN ACCORDANCE WITH THE RIGHTS OF INDIVIDUALS. This means that individuals must be informed, upon request, of all the information held about them, free of charge.
- IT IS KEPT SECURELY. This means that only staff and Councillors can access the data, it should be stored securely so it cannot be accessed by members of the public.

COLLECTING DATA
WPC recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of information. If, for example, a member of the public gives their phone number to staff or a member of WPC, this will only be used for the purpose it has been given and will not be disclosed to anyone else.

STORING AND ACCESSING DATA
WPC may hold information about individuals such as their addresses and telephone numbers. These are kept in a secure location at the Parish Clerk's place of residence and are not available for the public to access. All data stored on a computer is password protected. Once data is not needed anymore, if it is out of date or has served its use, it will be shredded or deleted from the computer. The Parish Council is aware that people have the right to access any information that is held about them. If a person requests to see any data that is being held about them, ·- They must be sent all of the information that is being held about them ·- There must be explanation for why it has been stored ·- There must be a list of who has seen it ·- It must be sent within one month.

DISCLOSURE OF INFORMATION
If an elected member of the council, for example a councillor needs to access information to help carry out their duties, this is acceptable. They are only able to access as much information as necessary and it should only be used for that specific purpose. If for instance someone has made a complaint about over hanging bushes in a garden, a councillor may access an address and telephone number of the person who has made the complaint so they can help with the enquiry. They can only do this providing they represent the area that the subject lives in. However, before they access any sensitive information about a person, they would need consent to do this from the Data Protection Officer. Data should never be used for political reasons unless the data subjects have consented.

Confidentiality
WPC is a public body and will seek to carry out its business in a public and transparent way but, where there are good reasons for confidentiality that are agreed by WPC, business can be conducted in a way that is sensible to those issues. The press and public may be excluded although a confidential record of such transactions will be held by WPC.
Council staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential. If a data breach is identified the ICO must be informed and an investigation will be conducted.

Data Protection Principles
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Handling of personal information

WPC will, through appropriate management and the use of criteria and controls:-

- Observe conditions regarding the fair collection and use of personal data;
- Meet its legal obligations to specify the purpose for which the information is used;
- Ensure the quality of information used;
- Apply checks to determine the length of time information is held;
- Take appropriate measures to safeguard personal information;
- Ensure the rights of people about whom the information is held can be fully exercised under the Act;

These include: The right to be informed that processing is being undertaken; the right of access to one's personal information within the statutory 30 days; the right to correct, rectify, block or erase information regarded as wrong information.

Sensitive Personal Information

The Parish Council does not process sensitive personal information.

Protecting Personal Information

- Employees and Council Members (Parish Councillors) acting on behalf of the Parish Council shall protect personal information in scope of this policy in accordance with the following:

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

2) Personal mobile devices and removable storage used by the Clerk, other staff and councillors. Councillor's mobile devices that are capable of storing personal information and/or sending and receiving email should secure those devices using a PIN or other device security facility to prevent unauthorised access to personal information should the device be stolen, passed on or otherwise compromised.

3) Physical Security of electronic and paper-based information held by the Clerk, other staff and councillor places of residence. All reasonable steps to secure information in the residence should be taken. Information of a sensitive nature, including but not limited to financial documents, cheque books and banking credentials should be physically locked away in a secure manner.

4) Use of externally hosted services (email, cloud storage services) External services and email accounts shall be secured with a strong password to prevent access to the account from remote devices.

5) Disposal of personal information when no longer required Personal information stored electronically shall be deleted from the appropriate applications, including deletion from the 'Recycling Bin' and reasonable endeavours to remove all copies and backups. (Records

may persist in electronic backups for long periods. These records are only accessed in exceptional circumstances and any out of data personal records shall be deleted at the point they are discovered in backup records.) Personal information in printed form shall be disposed of in such a way that the information cannot easily be reconstituted, for example by shredding or burning.

Implementation

The Clerk to WPC is responsible for ensuring adherence with the Data Protection Act and General Date Protection Regulation.

This policy will be reviewed annually, as well as an annual review of the compliance and effectiveness of the policy.

Approved by Watchfield Parish Council on 15.02.2022