# Warcop Parish Council – Data Protection Policy and Procedures

## Introduction

**The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR)** govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The Parish Council will remain the data controller for the information held. The Clerk and Councillors are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR.

### The Data Protection Act

The Data Protection Act contains 8 principles for processing personal data:

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s).
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure so as to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. 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.

#### Applying the Data Protection Act within the Parish Council

Warcop Parish Council will only collect personal data for the purpose of properly serving the Parish and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to the Clerk and the Councillors.

#### Correcting data

Under the Data Protection Act, individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where it is held, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress. Any SAR so received must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing them with information.

## Policy Statement and Purpose

Warcop Parish Council is committed to a policy of protecting the rights and privacy of individuals. Warcop Parish Hall needs to collect and use certain types of data, typically names and addresses, telephone numbers and bank account details, in order to effectively manage activities at Warcop Parish Hall**.** This personal information will be collected and handled securely.

The purpose of this policy is to set out the Warcop Parish Council commitment and procedures for protecting personal data. The 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 with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

### Responsibilities

**Warcop Parish Council** is the Data Controller under the Data Protection Act, and is legally responsible for complying with the Act, which means that it determines what personal information will be held and the purposes for which it is held.

The **Council** will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

1. Collection and use information fairly.
2. Specify the purposes for which information is used.
3. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
4. Ensure the quality of information used.
5. Ensure the rights of people about whom information is held, can be exercised under the Act.

**These include:**

1. The right to be informed that processing is undertaken.
2. The right of access to one’s personal information.
3. The right to prevent processing in certain circumstances, and
4. the right to correct, rectify, block or erase information which is regarded as wrong information.
5. Take appropriate technical and organisational security measures to safeguard personal information,
6. Ensure that personal information is not transferred abroad without suitable safeguards,
7. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
8. Set out clear procedures for responding to requests for information.

**The Council will be responsible for ensuring that the policy is implemented and will have overall responsibility for:**

1. Everyone processing personal information understands that they are contractually responsible for following good data protection practice
2. Everyone processing personal information is appropriately trained to do so
3. Everyone processing personal information is appropriately supervised
4. Anybody wanting to make enquiries about handling personal information knows what to do
5. Dealing promptly and courteously with any enquiries about handling personal information
6. Describe clearly how Warcop Parish Council handles personal information
7. Will regularly review and audit the ways it holds, manages and uses personal information
8. Will regularly assess and evaluate its methods and performance in relation to handling personal information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Chair of the Parish Council.

### Procedures for Handling Data & Data Security

Warcop Parish Council has a duty to ensure that appropriate technical and organisational measures are taken to prevent:

* Unauthorised or unlawful processing of personal data
* Unauthorised disclosure of personal data
* Accidental loss of personal data

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

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone’s name in a document comprises personal data; however, combining various data elements such as a person’s name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

### Operational Guidance – Data Protection Good Practice

**Email:**

The Clerk and Councillors should consider whether an email (both incoming and outgoing) containing personal information will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

**Phone Calls:**

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

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

**Laptops and Portable Devices:**

All laptops and portable devices that hold data containing personal information must be protected with a suitable password.

Ensure the laptop is locked (password protected) when left unattended, even for short periods of time. When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep the laptop or portable devices with you at all times, do not leave it in luggage racks or even on the floor alongside you.

**Data Security and Storage:**

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Always lock (password protect) your computer or laptop when left unattended.

**Passwords:**

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

* Common sense rules for passwords are: do not give out your password
* Do not write your password somewhere on your laptop
* Do not keep it written on something stored in the laptop case.

**Data Storage:**

Personal data must be stored securely and only accessible to authorised volunteers or staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

**Information Regarding Councillors or Former Councillors:**

Such information will be kept indefinitely. If something occurs years later it might be necessary to refer back to check what was disclosed earlier, in order that Councillors comply with their obligations.

**Data Subject Access Requests:**

Warcop Parish Council may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the Council and Parish. The circumstances where the law allows the Council to disclose data (including sensitive data) without the data subject’s consent are:

1. Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person e.g. child protection
2. The Data Subject has already made the information public
3. Conducting any legal proceedings, obtaining legal advice or defending any legal rights

**Risk Management:**

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. The Clerk and Councillors should be aware that they can be personally liable if they use customers’ personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

***Approved for use by Warcop Parish Council at an ordinary Meeting on 18/09/2025***