

# Cornwall VW Owners Club

## Data Protection Policy



### Data Protection Policy

#### Context and Overview

#### Key Details

- Approved by The Committee:
- Policy became operational on:
- Next review date: AGM 2018

#### Introduction

Cornwall VW Owners Club needs to gather and use certain information about its members. These can include member, spouse, children, and vehicle details.

This policy describes how this personal data must be collected, handled and stored to meet CVWOC's data protection standards – and to comply with the law.

#### Why this policy exists

This data protection policy ensures CVWOC:

- Complies with data protection law and follows good practice
- Protects the rights of all its members and their families
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

#### Data protection law

The General Data Protection Regulation 2016 describes how organisations – including CVWOC must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not to be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

## **People, risks and responsibilities**

### **Policy scope**

This policy applies to:

- All members of the Cornwall VW Owners Club
- All contractors, suppliers and other people working on behalf of CVWOC

It applies to all data that the club holds relating to individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

### **Data protection risks**

This policy helps to protect CVWOC from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the club uses data relating to them.

### **Responsibilities**

The committee and volunteers may have some responsibility for ensuring data is collected, stored and handled appropriately.

However the committee is ultimately responsible for ensuring that CVWOC meets its legal obligations.

The Membership Secretary as the data controller will also assume the role of Data Protection Officer.

- Keeping the committee updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Dealing with requests from individuals to see the data the club holds about them (also called subject access requests).

### **General guidelines**

- The only person able to access the data covered by this policy should be the membership secretary, who can pass the data to committee members who require it for specific tasks.
- Data should not be shared informally. When access to confidential information is required, members can request it from the membership secretary.
- All members should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular strong passwords should be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the club or externally.
- Data should be regularly reviews and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Members should request help from the data protection officer if they are unsure about any aspect of data protection.

### **Data storage**

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept as secure as possible.
- Members should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data when necessary should be protected by strong passwords that are changed regularly
- If data is stored on removable media (like a CD or DVD), these should be kept as secure as possible

### **Data use**

Personal data is of no value to the club unless the club can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- Personal data should not be shared informally.

- Personal data should never be transferred outside the European Economic Area
- Personal data should never be given to third parties.

### **Data accuracy**

The law requires CVWOC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort CVWOC should put into ensuring its accuracy.

It is the responsibility of the Membership Secretary to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary.
- CVWOC will make it easy for data subjects to update the information CVWOC holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored email, it should be removed from the database.

### **Subject access requests**

All individuals who are the subject of personal data held by CVWOC are entitled to:

- Ask what information the club holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the club is meeting its data protection obligations.

If an individual contact's the club requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Membership Secretary at [membership@cornwallvwoc.com](mailto:membership@cornwallvwoc.com).

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

### **Disclosing data for other reasons**

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CVWOC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the committee where necessary.

### **Providing information**

CVWOC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the club has a privacy statement, setting out how data relating to individuals is used by the club.

