

# **Data Protection Policy**

This policy will be reviewed annually or when there is a legislative change or review due to lessons learned or best practice guidelines

# Introduction

This policy addresses the Club's responsibilities under the UK General Data Protection Regulation (UK GDPR) 2016 and the Data Protection Act (DPA) 2018.

# **Definitions**

Ludlow Castle Motor Club Ltd (the Club) holds personal data about members and suppliers for a variety of purposes. This policy sets out how we seek to protect personal data and ensure that officers of the Club understand the rules governing their use of personal data to which they have access in the course of their duties.

Purposes for which personal data may be used by us include the following:

- Compliance with our legal and governance obligations and good practice
- Ensuring privacy policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, distribution of information and Club promotions
- Investigating complaints
- · Access to administrative information
- Improving services to Club members

#### Personal data

This includes information relating to existing or former Club members and suppliers. Personal data we gather may include individuals' name, address, contact number and email address.

# Sensitive personal data

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings is not requested, sought or held by the Club.

# **Scope**

This policy applies to all officers and members of the Club. You should be familiar with this policy and comply with its terms. This policy supplements any other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be distributed to members.

# Who is responsible for this policy?

The Club is not required to appoint a Data Protection Officer. The responsibility for this policy rests with the Club and is maintained and administered by the Club Secretary as the Data Collection Officer (DCO).

## **Our Procedures**

#### **Fair and Lawful Basis**

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to us doing so.

#### The Data Collection Officer's (DCO) Responsibilities

- Keeping the Club updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis

- Arranging data protection guidance and advice for all Club members and those included in this policy
- Answering questions on data protection from members and suppliers
- Responding to individuals such as members and suppliers who wish to know what data is being held on them by the Club
- Checking and approving with third parties that handle the Club's data any contracts or agreement regarding data processing

#### Responsibilities of the DCO or his/her Designate

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the Club is considering using to store or process data
- Approving data protection statements attached to emails and notices

### The processing of all data must be:

- Necessary to deliver services to our members
- In our legitimate interests and not unduly prejudice the individual's privacy

#### **Accuracy and Relevance**

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. Individuals may ask that we correct inaccurate personal data relating to them.

#### **Members' Personal Data**

The Club must take reasonable steps to ensure that personal data we hold about our members is accurate and updated as required. For example, if a member's personal circumstances change, they should inform the DCO so that the data can be updated in the Club's records.

# **Data Security**

The Club must keep personal data secure against loss or misuse. Where other organisations process personal data on our behalf, the DCO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

#### **Storing Data Securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Spreadsheets that hold member information should be password protected
- Data stored on memory sticks must be locked away securely when they are not being used
- The DCO must approve any cloud service used to store data
- Data should be regularly backed up in line with the Club's back up procedures

#### **Data Retention**

The Club must not retain an individual's data for longer than is necessary. 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 data retention guidelines or with the individual's consent.

# **Subject Access Requests**

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This requirement is included in the UK GDPR 2016 and is expected to be included in the DPA 2018 Act.

Subject access requests from individuals should be referred immediately to the DCO. There are also restrictions on the information to which individuals are entitled under applicable law.

#### Processing Data in Accordance with the Individual's Rights

The Club will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DCO about any such request. The Club will not send direct marketing material to someone electronically (e.g., via email) unless we have consent in relation to the medium of communication.

#### **Training**

The Club will ensure at all times that those with specific responsibilities under this policy will have access to the relevant training, and in the event of any changes to the policy or statute will be required to and be able to evidence that appropriate training has been undertaken.

# **Privacy Notice**

The Club has a Privacy Notice which identifies who the data controller is, with contact details for the Data Collection Officer/Club Secretary.

#### The notice:

- Sets out the purposes for which we hold personal data
- Highlights that our work may require us to give information to third parties
- Provides that people have a right of access to the personal data that we hold about them

Being transparent and providing accessible information to individuals about how we will use their personal data is important to the Club. The following are details on how the Club collects data and what we will do with it:

#### What information is being collected?

The Club collects data via the website contact form (name and email address). We also collect data via electronic or paper forms (name, email, telephone number, address) for our membership systems.

#### What is the data being used for?

In relation to the online contact form the data is only being transferred to a designated email address, it isn't being stored on the site. Data for membership system is used to contact club members regarding events, membership renewals and general Club marketing.

#### Who is handling the data?

The Data Collection Officer, the website administrators and officers of the Club.

#### How is the data collected?

All data is obtained by being submitted through a form. No data will be obtained without notification that it is being stored or without permission to do so.

#### How and where is the data stored?

In relation to the contact form the data is being stored in the designated email's mailbox. For the user login section, the data is being stored in the website database. Other data is stored on the Club's internal database under the name of each member.

#### Identity and contact details of any data controllers

The DCO is the sole administrator.

#### **Conditions for processing**

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All officers who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data within the privacy notice.

#### **Justification for Personal Data**

The Club will process personal data in compliance with all eight data protection principles.

#### Consent

The data the Club collects is subject to active consent by the data subject. This consent can be revoked at any time.

#### **Data Portability**

Upon request, a data subject should have 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.

# Right to be Forgotten

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.

#### **Privacy by Design and Default**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DCO will be responsible for conducting Privacy Impact Assessments, if applicable.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

#### **International Data Transfers**

No data may be transferred outside of the EEA without first discussing it with the DCO. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

#### **Data Audit and Register**

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

#### **Reporting Data Breaches**

All officers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures

#### **Monitoring**

All Club members must observe this policy. The DCO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

# **Consequences of Failing to Comply**

The Club take compliance with this policy very seriously. Failure to comply puts both members and the Club at risk. This may include identity theft when confidential information is exposed to unauthorised individuals or an infringement of the UK GDPR which may see the Information Commissioner's Office take action including the possibility of imposing a large fine. If you have any questions or concerns about this policy, please contact the DCO.