**Chorley Advanced Motorists Data Protection and Privacy Policy**

**Scope and limitations**

This policy applies to all personal data handled, stored and processed by Chorley Advanced Motorists (CAM).

**Purpose**

The primary purpose of this policy is to outline how CAM should handle, store and transmit personal data in order to ensure appropriate measures are taken to protect data in line with risk.

**Data Set information and definition**

In simple terms, data is information which is:

1. being processed by a computer
2. is being recorded in order to be processed by a computer
3. is a paper based record

This policy is only concerned with data which is defined as Personal Data:

‘’Data which relates to a living individual who can be identified:

1. from that data, or
2. from that data and other information which is in the possession of, or is likely to come into the possession of, the controller,

and includes any expression of opinion about the individual and any other person in respect of the individual’’

This also includes Sensitive Personal Data which includes:

1. racial or ethnic origin
2. political opinions
3. religious beliefs or other beliefs
4. trade union membership
5. physical or mental health or conditions
6. sexual life
7. the commission or alleged commission by the data subject of any offence
8. any proceedings for any offence committed or alleged to have been committed by the data subject.

The data controller in this case is CAM. No data processors are used by CAM to process data on our behalf.

CAM handles, stores and protects (collectively defined as processing) the following Personal Data Sets:

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Set** | **Type** | **Responsibility** | **Description** |
| Membership and benefactors list | Electronic spreadsheet, paper based forms recorded in filing system | Treasurer, Chairman | Contains information about current members and benefactors. Personal data held: name, address, contact details, IAM membership number, membership status such as payment status gift aid details. |
| Observer list | Electronic spreadsheet.Electronic mailing list. | Course Co-ordinator,Training Team, Secretary, Chairman. | Contains information about current observers. Personal data held: name, address, contact details, training records. |
| Associate list | Electronic spreadsheet complied from data sent to the group contact by the IAM. Paper and electronic copy of associate details for the purpose of course co-ordination. Individual notification of an Associate to the Group Contact from the IAM | Course Co-ordinator, Secretary/Group Contact, Training Team, Chairman. | List of current and previous Associates and who they have been paired up with from the Course Co-ordinator. Personal data held: Name, address, contact details.  |
| Group Mailing List | Electronic spreadsheets | Treasurer, Secretary, Newsletter Editors. | Personal data held: Name address, email address. |

**Protection of Data**

In line with the risk posed to this data, all data identified as a personal data set must be secured as follows:

1. All electronic files must be stored on computers/laptops and should be protected by password protection or encryption.
2. All copies of personal data must be kept to a minimum.
3. Distribution of personal data files must be kept to a minimum.
4. Electronic personal information as defined above must be encrypted in transit. If personal data is being sent via email, it must be encrypted first, with a strong password. When transferring personal files using a USB drive, CD or other forms of removable data, these must be encrypted. Passwords must be sent separately, preferably by SMS or verbally and not in the same body of the email.
5. All information on computers/laptops must be backed up so that if one copy is lost, another can be retrieved. These back-ups must be current. This can be done in two ways:
6. a second copy can be held on a computer by another person (so long as it satisfies points 1) and 2( above).
7. a backup drive can be used and this must be encrypted in line with 4).
8. All electronic device handling personal data must:
	1. Have the latest patches applied within 1 month of release,
	2. be running anti-virus software that is kept up to date.
9. Any paper-based files defined as personal data above, must be kept in a secure filing system. ‘’secure filing system’’ means making sure unauthorised persons cannot easily access the files, e.g. kept in a locked filing cabinet.
10. Paper based files must be shredded or burnt when no longer required.
11. If Cloud based storage systems are used for personal data, confirmation must be received from the Cloud storage provider that their system is GDPR compliant.
12. Publication of personal data must be kept to a minimum.

Exceptions to the controls above can be sought and approved on a case-by-case basis by CAM Executive Committee and these exceptions will be recorded in the committee meeting minutes.

**Approval for Holding Personal Data and Publication.**

CAM needs to hold personal data for the reasons outlined below to maintain membership of CAM and provide advanced driver courses. Additionally, CAM would like to use member’s photographic images and limited personal data (name) for publication in our newsletter, website and promotional materials. This publicity data will be made available on the CAM website, via the Internet and therefore anyone

worldwide with Internet access may be able to access the data, for this reason CAM will not have total control of this data once published. Members and previous members can request their publicity data be removed and opt out of CAM holding this data by contacting the Data Controller – details are provided in the contact details below.

Members may request all data be removed, however, it should be noted that CAM requires some data for membership, therefore a request for complete deletion of data also means leaving CAM. We retain the right to keep certain data if it is required for legal/investigatory proceedings.

**Data Held and Destruction of Data and Removal of Records**

Should an individual request their records are destroyed, CAM will delete all information related to that individual, however their membership must also end as we must keep information about all members to track payment etc.

Records must be destroyed after the following periods:

|  |  |  |
| --- | --- | --- |
| Data held | Retention period for personal data | Exceptions |
| Membership and benefactors list | Up to three years after the individual has left the group. Individual records are to be deleted as required | Unless member requests their data be removed. Retained for longer if subject to legal/investigatory proceedings. |
| Observer lists | Delete once used | Can be re-obtained from the IAM DTE as required. |
| Associate lists | Up to three years | Unless the associate requests their data be removed. Retain for longer if there are any ongoing legal/investigatory proceedings. |
| Group mailing List | Ongoing document. Individuals requesting their data be removed from our records would be removed from this list immediately. |  |

**Incident Process**

If a data breach is identified, then the Data Controller must be contacted as soon as is practical. The Data Controller will review the breach to determine if CAM is required to inform the Information Commissioner (ICO).

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Chorley Advanced Motorists are required to notify the ICO within 72 hours if, when a personal data breach has occurred, it has been established that it’s likely that there will be a risk to people’s rights and freedoms; if it is unlikely, then it doesn’t have to be reported. However, if the Executive Committee decides it doesn’t have to report the breach, then this must be documented along with the reason why that decision was made.

**Contact details**

For any queries or questions about this policy, please contact: secretary@chorleyiam.com

This email address is also to be used for subject access requests and requests to delete data from the CAM records.