SLAM Data Protection and Privacy Policy

Document Control

Version	Date	Author	Comments
0.1	02/05/2018	Jon Wallwork	First draft
0.2	22/05/2018	Jon Wallwork	Updates to approval section.
0.3	23/05/2018	Jon Wallwork	Updates to data held following May 2018 committee meeting.
0.4	13/04/2023	Dave Little	Removal of additional lists following data consolidation and adoption of MailChimp as database master.
0.5	25/10/2023	Ashley St John Claire	Update of Website hosting, Whatsapp, Googledrive and generic Data Controller contact.

Scope and Limitations

This policy applies to all personal data handled, stored and processed by South Lancashire Advanced Motorcyclists (SLAM).

Purpose

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

Data Set Identification and Definition

In simplistic terms, data is information which is:

(a) being processed by a computer
(b) is being recorded in order to be processed by a computer
(c) is a paper based record

This policy is also only concerned with data which is defined as Personal Data:
"Data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those 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 indication of the intentions of the data controller or any other person in respect of the individual"

This also includes Sensitive Personal Data which includes:

(a) Racial or ethnic origin
(b) Political opinions
(c) Religious beliefs or other beliefs of a similar nature
(d) Trade union membership
(e) Physical or mental health or condition
(f) Sexual life

(g) The commission or alleged commission by the data subject of any offence
(h) Any proceedings for any offence committed or alleged to have been committed by the data subject.

The Data Controller in this case is SLAM. No Data Processors are used by SLAM to process data on our behalf.

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

Data Set	Type	Responsibility	Description
Membership and benefactors list	MailChimp cloud based database	Membership Secretary, Course Coordinator, Chairman	Contains information about current members and benefactors. Personal data held: Name, address, contact details, IAM number, membership details such as payment status
Observer List	Electronic spreadsheet. Excel format.	Observer Coordinator, Chairman	List obtained as required from IAM DARTS website and then destroyed once used. Used to provide group and course coordinator with current observer list for matching associates to observers.
Associate List	Electronic spreadsheet Excel format compiled from emails sent to the group contact by the IAM.	Course Coordinator, Group Contact, Chairman and observers.	List of current and previous associates and who they have been paired up with from the observing team. Personal data held: Name, email address, phone number and home town.
Ride Clinic Lists	Electronic spreadsheets Excel format compiled from email responses to the Ride Clinic email alias.	Ride clinic coordinator, participating observers.	One list of members who would like to participate in the ride clinics. One list of observers who are happy to provide the ride clinics to members. Personal data held: Name, email address, phone number, home town.

Group Mailing list	Mail Chimp cloud based database	Membership Secretary, Course Coordinator	List of email addresses of members and interested parties who receive SLAM News. Opt out handled by Mail Chimp or Mail Chimp Admin User. Personal data held: Names, address, email address
Observer Mailing list (this is a sub category of the main group list above.	Mail Chimp cloud based database	Observer Coordinator, Chairman	List of Observers email addresses so we can send mails to Observers. Opt out handled by Mail Chimp or Mail Chimp Admin User. Personal data held: Names and email address.
Social Ride Participant Lists	Hard copy (hand written)	Ride Leaders, Group Secretary	List of participants on official SLAM organised social rides for emergency contact details and cross checking to member status.
Social Ride / Committee discussion	Whatsapp contacts on hand held devices and home computers	Ride Leaders and TECs, Committee members, Ride Participants	List of participants, interest groups or committee members on SLAM related events to allow communication and sharing of photos & documents on specific SLAM topics.

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 or cloud based storage, but must be protected by password protection or (in the case of cloud based storage) end to end 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. This means that when you are sending personal files via email, you must encrypt them first e.g. using Winzip or 7Zip with a strong password.
This also means that when you are transferring personal files using a USB drive,

CD or other form of removable media, you need to encrypt the files. Passwords/passphrases must be sent separately and not in the same body of the email.

5) All information must be backed up so that if one copy is lost, another one can be retrieved. These back-ups must be current. This can be done in two ways:
    a. A second copy can be held on a computer by another person (as long as it satisfies points 1) and 2) above)
    b. A backup drive can be used and this must be encrypted in line with 3) above.

6) All electronic devices handling personal data must:
    a. Have the latest patches applied within 1 month of release
    b. Be running anti-virus software that is kept up to date with the latest signatures

7) Any paper-based files defined as personal data above, must be kept in a secure filing system. "Secure filing system" means making sure that unauthorized persons cannot easily access the files e.g. kept in a locked cabinet or a locked Top Box for data that needs to be transported on a ride-out.

8) Paper based files must be shredded or burnt when no longer required.

9) Cloud-based storage systems (e.g. MailChimp and Google Drive) may only be used when demonstrably GDPR compliant and where data is encrypted both in-transit and at rest.

10) 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 SLAM Committee and these exceptions will be recorded in Committee Meeting Minutes.

Approval for Holding Personal Data and Publication

SLAM need to hold personal data for the reasons outlined below to maintain membership of SLAM and provide advanced rider courses. Additionally, SLAM would like to use members photographic images and limited personal data (Names) for publication in our newsletter, website and Facebook pages/closed groups. This publicity data will be made available via the Internet and therefore anyone worldwide with Internet access may be able to access the data (for this reason SLAM 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 SLAM holding this data by contacting the data controller – details are provided in the Contact Details section below.
Members may request all data be removed however it should be noted that we require some data for membership therefore a request for complete deletion of data also means leaving SLAM. We retain the right to keep certain data if it is required for legal/investigatory proceedings.

Data held & Destruction of Data and Removal of Records

Should an individual request that their records are destroyed, SLAM 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 3 years after the individual has left the group. Individual records are deleted as required.	Unless member requests their data be removed. Retained longer if there are any ongoing legal/investigatory proceedings
Observer lists	Deleted once used	Can be re-obtained from IAM DTE website as required.
Associate lists	Up to 3 years	Unless associate requests their data be removed. Retained longer if there are any ongoing legal/investigatory proceedings
Ride clinic lists	Up to 3 years after the individual has left the group. Individual records are deleted as required.	Unless member requests their data be removed. Retained longer if there are any ongoing legal/investigatory proceedings
Whataspp	Messages, docs and photos retained up to 3 years after individuals have left group.	Deleted on committee members phone when leaving committee. Unless member requests their data be removed. Retained longer if there are any ongoing legal/investigatory proceedings
All Mailing Lists		Retained info as per Mail Chimp conditions. Member names removed on request however.

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 SLAM is required to inform the Information Commissioners Office (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.

We are required to notify the ICO within 72 hours if, when a personal data breach has occurred, we establish that it's likely that there will be a risk to people's rights and

freedoms; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to document the breach and the decision made.

Third-Party Providers of Services

SLAM use the following third-party services:

MailChimp:
For maintaining members lists and email services used for sending bulk emails to the group.
Survey Monkey:
For sending periodic surveys to members – uses the email list from Mail Chimp and therefore holds no personal data.
20i:
Hosted service provider used by SLAM to provide our website
https://www.slambikers.co.uk
Facebook:
For our social media presence, organising ride outs and for SLAM and motorcycling chat.
Googledrive:
For storing non personal data; ride-out routes and ride sheets.
Whatsapp
For Committee, Special interest group or Group ride activities

SLAM handle data on all these third-party services / sites in accordance with this policy but due to the nature of third party services data is also handled by the third parties. Their privacy/security polices can be found here:
https://mailchimp.com/about/security/
https://www.surveymonkey.com/mp/legal/privacy-policy/
https://www.20i.com/legal/20i-ltd-privacy-policy
https://www.facebook.com/full_data_use_policy
https://www. https://support.google.com/drive/answer/2450387?hl=en-GB
https://www.whatsapp.com/legal/privacy-policy

Contact Details

For any queries/questions about this policy, please contact: data@slambikers.co.uk.

This email address is also to be used for subject access requests and requests to delete data from SLAM systems. You can also let us know any changes in preferences in via our website contact page www.slambikers.co.uk/contact.