BRITISH MOTORSPORTS MARSHALS' CLUB LTD.

IT Acceptable Use Policy

This policy applies to everyone involved in any way with the British Motorsports Marshals Club (BMMC), irrespective of role or capacity. The policy is effective from the Date of Issue shown at the bottom of this page.

Statement of Intent

This Policy covers the security and use of all BMMC information systems, services and IT equipment, including but not limited to the use of email, video conferencing, databases and websites.

This policy applies to all information, in whatever form, relating to the Club's activities, and to all information handled by the Club relating to other organisations with whom we deal. It also covers all IT and information communications facilities operated by BMMC (or on its behalf, including by third parties.)

This policy should be read alongside the Data Protection Policy.

Policy Aims

The aims of this policy are to ensure the following are met whilst on BMMC business:

- Confidentiality – access to data shall be confined to those with appropriate authority.
- Integrity – Information shall be complete and accurate.
- Availability – Information shall be available and delivered to the right person, when needed.

BMMC will review this policy every two years, as well as following a major regulatory change.

This policy will be communicated to all our member's and organisations working on our behalf, on our external website, and made available to third parties.

Leadership Responsibilities

The Policy Owner, shown at the bottom of this page, is responsible for implementing this policy on behalf of the BMMC Directors who will monitor its effectiveness.

User Access Control

Everybody required to access BMMC IT systems will be provided with their own unique User ID and password and are accountable for their actions on those systems.

Individuals must not:

- Share passwords without the approval in writing of a Director and then only in emergency circumstances.
- Leave their computer unlocked and unattended if in a public place.
- Try to access data they are not authorised to see.
- Store BMMC data on equipment that does not belong to them.
- Share BMMC data outside of BMMC unless their role description involves sharing such data. Under exceptional circumstances sharing of data can be approved in writing by a National Officer.

Those working with other role holders must ensure that individuals are given clear direction on the extent and limits of their authority about IT systems and data.

Any personal data that is printed must be securely destroyed, e.g. shredded with a crosscut shredder. All printing should be kept to a minimum.

BMMC Policy Owner: Sean Clarke	Policy Ref: BMMC/008
Date of Issue: 1st July 2024	Date of Next Review: 1st June 2026

The Use of the Internet and email

Use of BMMC email is for club purposes only. Individuals must not

- Use email to harass or abuse.
- Send offensive data.
- Conduct personal business.
- Gamble.
- Distribute spam.
- Make statements on behalf of BMMC unless their role description involves making such statements e.g. Comms and Social Media.
- Infringe any copyright, trademarks or other intellectual property.

Unless their role description involves doing so, Individuals must not:

- Put any information relating to BMMC on social media or other public services.
- Alter any information about BMMC.
- Express publicly any opinion about BMMC.

Mobile Storage Devices

Data should normally be sent through the BMMC email system, through the use of shared files on a system that has been authorised by a National Officer or using a secure service.

Devices such as memory sticks or removable hard drives must only be used if no other secure method to transfer data is available and you have written approval from a BMMC National Officer.

BMMC owned devices

All software used on BMMC owned devices must follow the software supplier's licensing agreements.

If you have been supplied with a device by BMMC, when you leave your role, or on the request of the IT Coordinator, the device must be returned to BMMC.

Software

Individuals must ensure that they comply with the licensing requirements of all software and services used in connection with BMMC, for example Zoom, MailChimp etc.

Monitoring

No email sent or received through the BMMC's system is private. BMMC may randomly review messages that have been created, received or sent via email to ensure compliance with this policy, or to ensure the smooth running of the club during absences, or for security.

Individual's Responsibility for IT and IT Security

BMMC relies on our members using their own Phones, Tablets, PCs etc, to access our systems. BMMC will not mandate specific security products, but does expect that individuals will take all reasonable precautions, such as:

- Anti-Virus / Security solutions
- Device Password timeouts / locks
- Spam / Phishing checks, i.e. are emails/texts really from whom they appear to be? Is that website genuine?

If you suspect a security breach, report it to the IT Coordinator immediately.