

Brisbane Sporting Car Club



Information Management Policy

This Policy was last reviewed and updated on: **10 October, 2023**

Purpose

Brisbane Sporting Car Club Limited (BSCC, alternatively the Club) values and respects the privacy of the people we deal with. BSCC is committed to protecting your privacy and complying with the Privacy Act 1988 (Cth) (**Privacy Act**) and other applicable privacy laws and regulations.

This Information Management Policy supports the Club Privacy Policy, and details the specific approaches BSCC takes with information in its possession. The Information Management Policy further describes the management requirements for information collected for or on behalf of BSCC by third parties, and/or information transmitted to third parties by BSCC in the conduct of BSCC's activities.

Scope

This policy applies to all BSCC staff, suppliers, contractors, and Board members, and to volunteers assisting BSCC with activities run or supported by BSCC.

It applies to all information assets, in any format, created or received in the course of BSCC's business.

This document is a public document, available upon request to any interested party upon request.

Policy Statement

BSCC recognises information assets as valuable, and is committed to achieving appropriate and consistent management of these assets to advance BSCC's priorities. Further, BSCC recognises that some of the information in its possession is of significant value and relates to, or describes, BSCC members' or volunteers' personally identifiable information (PII).

Key Mandates and Principles

All parties covered by the scope of this document must take reasonable steps to protect PII according to the *Privacy Act 1988* and the Australian Privacy Principles¹. This includes the storage and management of personal information stored in cloud services or by third parties on behalf of BSCC.

For the purposes of this document, PII is one subset of information shared with or created by BSCC *in confidence*, and for the remainder of this document shall be referred to in conjunction with other Confidential Data, except where explicitly referenced.

In the context of this document, Confidential Data is any data which has been provided to, or created by, BSCC in the conduct of BSCC's activities, that if made available to the public through either act or omission would cause significant harm and/or reputational damage to BSCC, its office bearers, and/or other interested parties.

Those principles are summarised as follows:

- Confidential Data requested by or on behalf of BSCC must service a specific need in the conduct of BSCC's activities, with alternative approaches to the collection of that PII thoroughly scrutinised and excluded prior to its collection.
- Confidential Data stored by or on behalf of BSCC must be stored for the minimum reasonable time in the pursuit of BSCC's activities.
- Confidential Data stored must be stored in the minimum number of locations required in order to support BSCC's activities.
- Confidential Data stored must be accessed and accessible only by those individuals or entities with a reasonable, lawful purpose for access.
- Confidential Data stored must be deleted and/or corrected upon explicit or implicit request from the party to which the Confidential Data refers.

¹ <https://www.oaic.gov.au/privacy/australian-privacy-principles>

Creation and Management of Information Assets

For the benefit of clarity, some examples of Confidential Data follow:

- Information covered by a Non-Disclosure Agreement (NDA) with a third party.
- Personally-Identifying Information (PII) of any type, of any member of or volunteer to BSCC.
- Commercial and/or financial records, other than those required to be available to the public and/or membership by law.

This list is non-exhaustive, and individuals covered by the scope of this document are expected to exercise reasonable judgment in determining whether particular information would meet the definition described above.

Information Assets not meeting the definition of Confidential Data should be managed in accordance with principles of reasonable judgement, and otherwise in consistency with the tenets and principles covered in this document.

Information Management System

The Information Management System (IMS) in use by BSCC consists of the Microsoft 365 suite of tools, including but not limited to Forms, OneDrive, Teams, Word, Outlook, and Excel. This consists of a subscription ("tenancy"), domiciled in Australia, in which BSCC stores all relevant information.

Accounts in the IMS tenancy shall be provided by BSCC to individuals covered by this Policy, where required for those individuals in order that they comply with this Policy. Where these are provided, individuals are required to utilise their own accounts to access the IMS tenancy. Under no circumstances are users to share accounts with any other individual, whether that individual is otherwise authorised to access Confidential Data or not.

Data Access, Retrieval, and Creation

Wherever Confidential Data is created by or provided to BSCC, alternatives to the provision of that data shall have been explored and excluded, such that the provision of that data is the only reasonable approach in the conduct of BSCC's activities.

Wherever Confidential Data is created by or provided to BSCC, only the minimum data required such that BSCC can conduct its activities efficiently and effectively shall be created, provided, and stored by BSCC.

Computers used to access Confidential Data shall use web based access to the IMS, with the sole exception of the BSCC's office computer/s and other BSCC-owned assets, which may utilise on-device versions of the IMS applications.

The BSCC's computers shall be configured to use device encryption such as BitLocker or other equivalent. It is strongly recommended that this standard apply to all computers used to access Confidential Data, even where web based access is utilised.

Access to Confidential Data shall be logged, with audit records available through the IMS.

It is recognised that the BSCC conducts activities in locations where web-based access is infeasible. Where this is the case, the minimum Confidential Data required to conduct those activities shall be provisioned on either paper copy or an appropriately secured computer, and destroyed once no longer required for that activity. Such copies shall be handled with appropriate privacy protection, and collated in a manner so as to afford minimal risk of loss. Destruction methods of hard copies shall render the content unreadable; a cross-cut shredder or incineration are preferred methods.

Data Storage

Where required by law, data required for long term storage shall be flagged as such in the appropriate IMS tool/s, and deletion protection shall be enabled for that data. In this circumstance, data shall be stored for the length of time required by law, and destroyed once all relevant legal obligations have been met.

Brisbane Sporting Car Club

Confidential Data shall be destroyed as soon as it is no longer required. No deletion protection shall be utilised under any circumstances for Confidential Data, except where required by law as noted above.

All copies of Confidential Data stored by any party covered by this Policy, which has been created or retrieved at any time in support of BSCC's activities, shall be destroyed by those third parties upon request by an authorised officer of BSCC.

Data Transfer

Wherever reasonably feasible, Confidential Data created by or provided to BSCC shall be created, and subsequently reside, in BSCC's IMS tenancy to the exclusion of all other systems.

Where this is not possible, such as with a third party system which relies on email for dissemination of Confidential Data, that data will be imported and/or exported from the BSCC IMS tenancy in the shortest number of steps feasible.

For example, a third party system operating with BSCC member PII, such as the Motorsport Australia Event Portal, may rely on email as a mechanism by which PII is shared with BSCC. In this example, the third party system must be configured to send and/or receive emails from the BSCC's IMS tenancy rather than relying on individuals' personal email accounts.

In another example, a Sponsor may provide commercial-in-confidence material to BSCC on a USB thumb drive. In this example, the Confidential Data must be uploaded to the BSCC IMS as soon as practicable, and then the contents of the thumb drive erased.

Wherever possible, these types of arrangements in the examples above shall be avoided, and used as a last resort only, noting BSCC's responsibility for Confidential Data does not necessarily cease beyond BSCC's custody of that data.

Wherever Confidential Data is created by or provided to BSCC and is expected to be provided to a third party, alternatives to the provision of that data shall have been explored and excluded, such that the provision of that data is the only reasonable approach in the conduct of BSCC's activities.

Where BSCC must make Confidential Data available to a third party in order to conduct BSCC's activities, BSCC must take reasonable steps to ensure that the third party complies with BSCC's Information Management Policy and Privacy Policy as amended from time to time, or complies with their own Privacy Policy to a standard equal to or higher than that of BSCC's Privacy Policy.

Where BSCC must make Confidential Data available to a third party in order to conduct BSCC's activities, only that data absolutely necessary in order to conduct those activities is to be shared with the third party.

Nothing in the above statements should be interpreted as precluding BSCC from complying from reasonable, lawful requests for Confidential Data, such as those issued by a court of law, or those issued by a subject of PII consistent with the BSCC's Privacy Policy.

Data Format

Data created, retained, stored, transferred, and utilised by BSCC should be retained in the format/s native to the IMS, or in a generally available open standard format. The use of proprietary readers to access information is explicitly discouraged, except where no alternative option reasonably exists.

Roles and Responsibilities

All BSCC staff, contractors, suppliers, Board members, and volunteers have responsibilities to adhere to this Information Management Policy to the greatest extent reasonably feasible.

The BSCC Board have a specific responsibility to ensure that this Information Management Policy is upheld by all relevant parties, and that it reflects current best practices and BSCC's intended actions as pertains to information in BSCC's possession.

The BSCC Board have a responsibility to nominate a Data Custodian, who has the specific responsibilities of:

- ensuring, to the greatest extent possible, that all parties subject to this Information Management Policy comply with the Information Management Policy;
- ensuring, to the greatest extent possible, that all parties subject to this Information Management Policy have the tools and training in order to comply with the Information Management Policy;
- being the first point of contact for any queries relevant to this Information Management Policy or the BSCC's Privacy Policy; and
- being the first point of contact for any remediation required in order to maintain compliance with this Information Management Policy.

Communication and Training

This policy will be communicated to all interested parties, with a briefing on its content and intent to be provided upon request at any time, and specifically whenever an individual is granted access to the BSCC IMS.

Monitoring and Review

This document is to be reviewed annually, with the next review to occur no later than **1 June, 2024**. This document was first adopted by BSCC on **10 October 2023**.

Compliance with the principles of this document will be subject to logging and audit, where required to comply with the Privacy Policy.


Resources

The Club Data Custodian is **Iain ROBERTSON**, and is contactable at data@bscc.asn.au.

Motorsport Australia's Privacy Policy is accessible at [motorsport-australia-privacy-policy3d9fb9f070314f1394c9851710b37192.pdf](https://www.motorsport-australia-privacy-policy3d9fb9f070314f1394c9851710b37192.pdf).

Statement of Assent

This document has been reviewed by the BSCC Board, and accepted on **10 July, 2023**.



Tony Kabel
President
Brisbane Sporting Car Club
10 October 2023