SINGAPORE SPORT INSTITUTE INSTITUTIONAL REVIEW BOARD – Data Management Policy

This document aims to guide all researchers under the purview of the Singapore Sport Institute – Institutional Review Board (SSI-IRB) on proper data collection, storage and maintenance, and sharing methods, taking reference to the Sport Singapore – "*Data Management Policy V1.1*".

Specifically, in the governing of:

1. Data Collection

Data users will:

1.1. **not** obtain more personal information beyond what is reasonable for purpose of the research.

1.2. **not** obtain the consent through deception or by providing misleading or incomplete information.

1.3. take into account the type of data, its sensitivity and the circumstances to determine the appropriate form of consent to use.

1.4. obtain consent directly from the individual or an authorised representative (such as a legal guardian or a Person having power of attorney) unless requirement for consent is waived by the SSI-IRB.

1.5. obtain consent at or before the time of processing. Unless the purpose for the use of data was not previously identified, consent may be obtained after the data is collected but before use. (Retrospective Application)

1.6. anonymize all data from the instance of data capture and collection by means of arbitrary participant coding (i.e. 001, 002, etc.) in the specific format as listed in Figure 1; and storing the identification data in a password-protected document (refer to Section 2).

Document Classification: CONFIDENTI

	A	B	C
1	**Serial**	**Participant Name**	
2	001	Peter Tan	
3	002	Mary Lee	
4	003	John Ang	
5	004	Joseph Goh	
6	005	Tan Ah Lian	
7	006	Nicholas Lee	
8	...		

Figure 1. Format for participant coding

2. Data Storage and Maintenance

Data users will ensure that they protect Personal Data to minimise unintended disclosure by:

2.1. strictly prohibiting anyone from storing identifiable data on personal laptops or devices

2.2. using strong password[a] to secure a collection or compilation of Personal Data stored in electronic file[b], **within an encrypted thumb-drive**; no document containing personal data should be stored unprotected by a strong password.

2.3. limiting access, via the encrypted thumb-drive, to identifiable information to only the Principal Investigator (PI) and Co-PI. The PI and Co-PI may have access to the encrypted thumb-drive for as long as required (see section 2.4). **Serious disciplinary and legal actions will be taken against the PI and Co-PI in the event of breach in PDPA.**

2.4. transferring, for safekeeping, all identifiable personal data **immediately** after completion of data collection and, only in the specific case of servicing a sport, after provision of feedback to the relevant parties, to the appointed SSI-IRB data management officer (DMO); from which point onwards, only the appointed DMO will have access to the identification data document. Temporary access to the identification document can be granted to the PI of the respective research upon approval by the SSI-IRB secretariat team.

2.5. storing all data and documents pertaining to the research within the designated SSI-IRB research cabinet under lock and key for a minimum of 7 years, accessed via the DMO.

3. Data Sharing

Data users will:

3.1. use data for its intended purposes only.

3.2. share only anonymized data amongst research team.

3.3. **not** share identifiable data with any external parties (e.g. Coach) not involved in the research unless stated in the signed and approved informed consent form; sharing of identifiable data with Co-PI is subjected to a signed and approved Research Collaboration Agreement.

3.4. in the event of an incidental finding during data analysis, data users are permitted to re-identify and inform the research participant of this finding.

The current appointed Data Management Officer for SSI-IRB is: _____

To which the following responsibilities are assigned:

1. Ensure proper safekeeping of physical key to designated SSI-IRB metal cabinet
2. Ensure proper safeguarding, through multi-layered protection, of sensitive personal information/data obtained for and through research.
3. Act as a gatekeeper strictly preventing access of identifiable data to anyone, unless authorized by SSI-IRB secretariat team.

The above guidelines are written to assist researchers in ensuring proper research data management. They seek reference from the Sport Singapore "Data Management Policy V1.1" but do not, by any means, represent the referenced policy.

Responsibility lies on the researchers to maintain the abovementioned minimal standards and ensure the integrity of their participants' information. Failure of which can result in disciplinary actions by Sport Singapore and, to the extent of, the Ministry of Health.

---

[a] Ref: strong password guidelines – https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/secure-your-password;

[b] Electronic file refers to excel spreadsheet, word document, etc. ICT systems with appropriate access controls are considered to have met the requirements of password protection.