SCHEDULE 2: HIGH PERFORMANCE DATA GOVERNANCE

DOCUMENT CONTROL

Name:	High Performance Data Governance Guidelines
Version:	1.0
Effective date:	1 July 2026
Review due:	30 June 2027
Owner:	Head of Performance Services
File location:	AMS and AC Performance Services ZenDesk
Document type (& enforceability):	Framework (contains mandatory obligations & best-practice recommendations)[1]
Responsible parties:	Heads of Performance Services / SSSM Managers; SSSM Practitioners; Analysts; Coaches; Operations staff
Beneficiaries:	All players; HP staff dealing with player data; AC organisations
Applicable setting:	Matches and all training environments; clinical environments; AC Ops team offices; camp and touring environments

RELATED DOCUMENTS & LINKS

Document Name	Location
Australian Cricket Cyber & Information Security Policy v6.4 (Feb 2025)	*cricket.com.au* and *ZenDesk*
Australian Sports Commission Best Practice Principles on Player-Centric Governance of Technology and Player Information (Data Governance)	*AIS Data Governance*
Australian Privacy Principles (Privacy Act 1988) and APP Guidelines	*Federal Register of Legislation: Privacy*
Australian Academy of Science: Getting Ahead of the Game – Player Data in Professional Sport" (2022)	*Australian Academy of Science report*
Cricket Australia My Health Record procedure	*ZenDesk*
Australian Cricket Research Guidelines	*SSSM Principles Schedule 16* and ZenDesk
Memorandum of Understanding between CA and the ACA (2023-2028)	*ZenDesk*

[1] It must be noted that this Framework provides guidance to support legal obligations within the Australian Cricket Cyber & Information Security Policy v6.4 (Feb 2025); Australian Privacy Principles (Privacy Act 1988) and APP Guidelines; and Memorandum of Understanding between CA and the ACA (2023-2028) are met. Though CA will not audit all elements of this Framework, it is strongly recommended AC organisations consider implementation of this Framework as essential.

1. PURPOSE

1.1 This Framework establishes player-centric, lawful, secure and ethical governance for all High Performance (HP) data within Australian Cricket (AC). It explains how AC looks after player data in High Performance programs.

1.2 This Framework implements AC's Cyber & Information Security Policy and the Australian Privacy Principles (APPs) and integrates Australian Sports Commission (ASC) Best Practice Principles on athlete-centric governance.

1.3 The principles outlined in this Framework are relevant to all schedules included in the SSSM Principles.

2. SCOPE

2.1 This Guideline applies to player information such as:

a) Names and contact details

b) Training load, GPS and movement data

c) Wellness and screening data

d) Injury and medical information

e) Physiotherapy and imaging reports

f) Nutrition and psychology information (where clinically appropriate)

g) Team selection, scheduling and availability information

2.2 This Guideline applies to systems such as:

a) Teamworks (AC's athlete management system)

b) Approved medical record systems (e.g. Medirecords)

a) Approved wearable and tracking systems (e.g. GPS)

b) Approved performance analytics platforms within AC's technology environment

2.3 This Guideline applies to people such as:

a) High performance staff

b) SSSM staff, analysts, and Player Development Managers (performance support staff)

c) AC employees, contractors, or external service providers

d) Coaches and selectors

e) Players (including pathways players)

3. DEFINITIONS

3.1 Player-centric governance means:

a) Player data belongs to the player, it does not belong to the organisation[2]

b) Australian Cricket acts as a custodian of player data

c) Decisions about data must always consider what is best for the player

---

[2] The player medical record is jointly owned by the doctor who wrote the record and the player

3.2 Sensitive player information includes:

a) Medical, health or injury information

b) Biometric and body data

c) Psychological or wellbeing information

d) Any data classified as highly sensitive under Australian Cricket standards

Sensitive player data must be handled with sensitivity and confidentiality, and only shared in alignment with the relevant clauses of the Memorandum of Understanding between CA and the ACA (2023-2028).

4. ALIGNMENT WITH OTHER POLICIES

4.1 This Guideline is built to align with:

a) Australian Cricket's Cyber & Information Security Policy

b) Australian privacy laws

c) National high-performance sport expectations

d) Guidance from the Australian Academy of Science on responsible athlete data use

e) Australian Cricket Research Guidelines

4.2 It must be noted that the legal obligations outlined within clause 7 are compulsory, and this framework takes a practical approach to guiding how Performance Service personnel can ensure compliance.

4.3 You do not need to know these documents in detail. This Guideline reflects what they require in practical terms.

5. GUIDING PRINCIPLES

Everything in this Guideline is based on the following principles:

5.1 *Players come first.*
Data exists to support players, not the other way around.

5.2 *Only collect data that is needed.*
If data does not clearly help health, safety or performance, it should not be collected.

5.3 *Be open and clear.*
Players must understand what is collected, why, and how it is used.

5.4 *Keep data safe.*
Strong security is required at all times.

5.5 *Use technology responsibly.*
Just because technology can collect something doesn't mean it should.

5.6 *Be accountable.*
Australian Cricket must be able to show it is managing player data properly.

6. ROLES AND RESPONSIBILITIES

6.1 CA Head of Performance Services (Guideline Sponsor)
Owns this Guideline; ensures HP practices and technologies comply with AC principles and CA standards; ensures player engagement and transparency.

6.2 CA Head of Platforms, Operations and Cyber Security (Control Owner)
Maintains cyber standards; monitors compliance; oversees incident response, supplier security and assurance activities.

6.3 CA Senior Manager, Performance Data & Technology
With Head of Performance Services, ensures HP practices and technologies comply with AC principles and CA standards.

6.4 CA Legal
Oversees APP compliance, layered notices/consents, DPIAs, cross-border disclosures, NDB notifications and privacy complaints handling.

6.5 Information Owners
Classify information, approve access, perform quarterly access reviews, ensure local adherence to retention and disposal. SSSM Managers (or equivalent) are the Information Owners for all performance and health-related data. Operations personnel are the Information Owners for personal and administrative data.

6.6 System Owners (Teamworks)
Configure SSO/MFA, RBAC and logging; manage integrations; maintain audit evidence; enforce platform rule and lifecycle controls.

6.7 Everyone
Comply with AC policy, guidelines and standards; report incidents and suspected non-compliance; complete training.

7. HANDLING OF PLAYER DATA

7.1 Why and how we collect data (Lawful Collection)

a) We only collect player data for clear reasons, such as:
   (I) Injury/illness management and rehabilitation
   (II) Training and competition preparation
   (III) Return-to-play decisions
   (IV) Monitoring workload and wellbeing

b) Players must be told:
   (I) What data is collected
   (II) Why it is collected
   (III) Who will see it
   (IV) How long it will be kept
   (V) What rights they have (including their ability to request access to, or removal of their data)

c) This information is explained clearly inside Teamworks. If a type of data is optional and sensitive, players must agree to it first.

7.2 Where sensitive player data can be handled (Platform Rule)

a) Sensitive player information must be shared and communicated through Teamworks (or Medirecords) only[3],[4]. This includes conversations, notes, attachments and updates about:
   (I) Injuries or illness
   (II) Medical status
   (III) Wellness
   (IV) Load management
   (V) Personal information

b) Sensitive data must not be shared using:
   (I) Email
   (II) Text messages
   (III) WhatsApp
   (IV) Personal messaging apps
   (V) Unapproved spreadsheets or local files

c) Select data may be stored in approved proprietary software systems (e.g. Catapult OpenField for GPS data) but the sharing and communication of data must follow the rules detailed above.

d) When engaging with external medical providers, player data will be captured and stored on external providers' own data platforms. Common examples include, but are not limited to:
   (I) Medical imaging providers;
   (II) Pathology clinics; and
   (III) Orthopaedic or other specialist medical or surgical clinics.

7.3 Who can see what (Access Control)

a) Player data access depends on role:
   (I) Medical staff: medical and clinical records
   (II) Clinical staff: clinical records as appropriate to domain expertise
   (III) Performance staff, coaches, selectors: training and performance data (not medical or clinical notes, other than summaries intentionally and appropriately made available within the Teamworks platform)
   (IV) Executives and operations staff: high-level summaries without personal health information (unless specific consent is obtained)

b) Access is only granted for the players, teams, squads or programs a person is engaged by AC to work with directly.

c) Access is reviewed regularly. When someone leaves a position, their access is removed immediately.

7.4 Keeping data safe (Security Control)

a) Australian Cricket protects player data by:
   (I) Encrypting data so others cannot read it
   (II) Monitoring who accesses or downloads data

---

[3] As per the Player Contracts, sensitive player information may be shared via other means (email, verbal, medical portal) with external specialists when external medical opinion or treatment is to be provided, always with the informed consent of the player.

[4] Some external cricket franchises may use less secure platforms for their athlete data management. Where this occurs, players must give consent for Performance Services staff to share player data with these teams via the most secure channels possible.

(III) Securing laptops, phones and tablets

(IV) Keeping safe backups in case systems fail

b) These protections are already built into Teamworks and approved systems.

7.5 Introducing new tools or analysis

a) Before using new technology, trackers or analysis:

(I) We check how it affects players

(II) We assess whether it is fair and justified

(III) We confirm it is secure

(IV) We ensure players can understand it

b) Where possible, player identifiers are limited. If models or analytics influence decisions, they must be explained in simple terms.

7.6 Sharing data outside Australian Cricket

a) Player health or body data must not be shared externally unless:

(I) The player provides specific consent, or

(II) The law requires it

b) Research and improvement projects must adhere to the AC Research Guidelines.

7.7 How long data is kept

a) Medical records are kept as required by law

b) When a player leaves the AC system:

(I) Access to their data becomes restricted

(II) Use of data requires approval from CA Head of Performance Services

c) Data will be stored for a minimum of 7 years from when the player leaves the AC system, or until the player is aged 25, whichever is later.

(I) Data with potential for longer-term benefit (e.g., group-level research) will be retained.

(II) Data with no potential longer-term benefit (e.g., personal contact details) will be securely destroyed.

7.8 If something goes wrong (Incident Response)

a) If player data is mishandled or accessed incorrectly:

(I) It must be reported immediately

(II) Australian Cricket will investigate

b) Players and regulators will be notified if there is a real risk of harm

c) Lessons are documented and improvements made.

7.9 External systems and suppliers

a) Any external provider handling player data must:

(I) Meet security expectations

(II) Protect data properly

(III) Allow checks if needed

(IV) Report any data issues immediately

b) Suppliers are reviewed regularly.

7.10 Exceptions

a) If a program cannot follow part of this Guideline:
    (I) A formal exemption must be approved
    (II) Risks must be documented