IT Policy Framework

Kotara South Football Club

Effective Date: 10 February 2026

Document Category: Policy – Information Technology

Document Control

Version	Date	Author	Owner	Approval	Remarks
1.0	6/11/2025	G Merrick	Kotara South Football Club	KSFC - Committee	10/02/2026

This comprehensive **IT Policy Framework** is tailored for an Australian non-profit sporting club.

This framework is designed to help you meet Australian compliance best practices, particularly regarding data privacy (Australian Privacy Principles), which is critical for sporting clubs due to the sensitive nature of information collected (member details, payment info, and potentially health/injury records).

1. Introduction and Purpose

This policy outlines the rules, procedures, and responsibilities for the proper use of Kotara South Football Club's Information Technology (IT) resources and the handling of club data.

- **Scope:** Applies to all Committee Members, Coaches, Volunteers, Contractors, and any individuals using the Club's IT resources or handling its information, including personal devices used for club business.
- **Goal:** To protect the Club's information assets, ensure compliance with Australian legislation (especially the **Privacy Act 1988** and the **Australian Privacy Principles [APPs]**), and maintain a professional and secure digital environment.

2. Data and Information Management

The Club collects and holds personal information about members, players, and volunteers (e.g., names, contact details, payment info, and health/injury information). Adherence to the APPs is paramount.

a. Privacy and Personal Information (Australian Privacy Principles – APP 11)

Policy Area	Detail
Collection & Use	Only collect personal information that is reasonably necessary for the Club's functions (e.g., registration, competition, injury management).
Consent	Obtain clear consent for collecting **sensitive information** (like health/injury data) and explain *how* the information will be used and disclosed (e.g., to coaches, league officials).
Data Security	All personal data must be stored securely, protected from misuse, loss, unauthorised access, modification, or disclosure. (See Section 3).
Access & Correction	Members have a right to access and correct the personal information the Club holds about them.
Data Retention	Personal information must be destroyed or de-identified when it is no longer needed for any legal or operational purpose.

b. Cloud Services and Third-Party Providers

- **Vetting:** Any third-party provider (e.g., registration software, accounting platforms, website hosting) must be assessed for their security practices and compliance with Australian privacy laws.
- **Data Location:** Prefer Australian-based cloud services. If data is stored overseas, a detailed risk assessment must be performed, and the individual must be made aware (APP 8).

3. Cyber Security and IT Asset Protection

a. Password Management and Authentication

- **Strength:** All Club accounts (including email and online platforms) must use strong passwords/passphrases (minimum 8 characters, mix of characters, or a combination of words).
- **Multi-Factor Authentication (MFA):** MFA must be enabled on all critical accounts, including email, banking, registration databases, and cloud storage.
- **No Sharing:** User accounts and passwords must never be shared. Shared accounts for functional roles (e.g., "clubtreasurer@...") must be avoided where possible.

b. Device and Software Management

- **Club-Owned Devices:** Must be protected with strong passwords or passphrases and up-to-date operating system/security software.
- **Personal Devices (BYOD):** If personal devices are used for Club business, the individual is responsible for keeping the device secure and removing all Club data upon ceasing their role.
- **Software:** Only licensed and approved software is to be installed on Club devices. Automatic updates for all operating systems and software must be enabled.

c. Email and Internet Use

- **Club Email:** The Club email system is for Club business. Users must use professional judgment and avoid sending sensitive information via unencrypted email.
- **Phishing/Scams:** Users must be trained to recognise phishing, spoofing, and other social engineering attempts. Suspicious emails should be immediately reported to the nominated IT contact**.**

4. Incident Response and Business Continuity

a. Data Backup

- **Routine Backups:** All essential Club data (e.g., membership lists, financial records, key documents) must be regularly and automatically backed up to a secure, off-site location (e.g., a reputable cloud service).
- **Testing:** Backups must be tested periodically to ensure data can be successfully restored.

b. Data Breach Response

A Data Breach Response Plan has been developed below in Appendix A.

Key steps include:

i. **Containment:** Isolate the affected systems immediately to stop further damage.

ii. **Assessment**: Determine the scope and severity of the breach, including the types of data affected and the individuals involved.

iii. **Notification:** If a breach is likely to result in **serious harm** to affected individuals, the Club has an obligation under the **Notifiable Data Breaches (NDB) scheme** to notify the Office of the Australian Information Commissioner (OAIC) and the affected individuals as soon as practicable.

5. Roles and Responsibilities

Role	Responsibility
Committee	Ultimate responsibility for adopting, implementing, and enforcing this policy.
IT Contact	Oversees day-to-day IT security, manages user access, and acts as the initial point of contact for incidents.
All Users (Volunteers/Coaches)	Read, understand, and comply with this policy. Report any suspected security incidents immediately.

Disclaimer: *This framework provides an outline based on best practices and Australian privacy principles for non-profits. It is **not legal advice**. You must have your final policy reviewed by an Australian legal professional to ensure it fully meets your specific legal and operational requirements, especially regarding the definition of 'sensitive information' and Notifiable Data Breach obligations.*

Appendix A – Data Breach Response Plan

Data Breach Response Plan

Purpose

To establish a clear, documented set of procedures for the Kotara South Football Club to follow in the event of any suspected or actual data breach involving personal information. This plan ensures compliance with the Australian Privacy Act 1988, particularly the Notifiable Data Breaches (NDB) scheme.

1. Plan Activation and Response Team

A data breach is defined as unauthorised access to, or disclosure of, personal information, or loss of personal information that is likely to result in unauthorised access or disclosure.

1.1 Immediate Action

Any volunteer, coach, or committee member who suspects a data breach **must immediately**:

i. **Do not delete or modify anything.**
ii. **Report the incident** to the designated IT Contact (or a Committee Member if the IT Contact is unavailable).
iii. **Provide all known details:** What happened, when it was discovered, and what information (e.g., email, system, paper file) is affected

1.2 Response Team

The following roles form the core Data Breach Response Team:

Role	Primary Responsibility
Response Leader	Club President or nominated Committee Member. Manages external communication and legal/regulatory compliance.
Technical Lead	Club IT Contact. Executes technical containment, evidence collection, and system recovery.
Communication Lead	Club Secretary or Marketing Officer. Manages internal and external notifications (members, media).

2. Stage 1: Containment (Stop the Spread)

The goal is to immediately limit the scope and impact of the breach.

Step	Action	Responsibility
2.1 Isolate System	Immediately take affected systems offline (disconnect from the network/internet) or revoke access credentials. **Do not turn off devices.**	Technical Lead
2.2 Revoke Access	Change or disable passwords/credentials for all accounts suspected of being compromised. If the breach involves phishing, change all shared club passwords.	Technical Lead
2.3 Preserve Evidence	Log and secure all forensic evidence (e.g., system logs, activity history) before making changes.	Technical Lead
2.4 Patch Vulnerability	Identify and close the pathway the attacker used (e.g., applying missing updates, fixing website security gaps).	Technical Lead
2.5 Inform Committee	Inform all Committee Members that a breach has occurred and contain internal communications to only those who need to know.	Response Leader

3. Stage 2: Assessment (Understand the Harm)

The goal is to gather facts and determine if the breach meets the threshold for mandatory notification under the NDB scheme (i.e., whether "serious harm" is likely)

Step	Action	Responsibility
3.1 Determine Information Type	Identify exactly what personal information was involved (e.g., names, phone numbers, player health records, financial details). **Sensitive information requires urgent attention.**	Response Leader / Technical Lead
3.2 Calculate Scope	Identify the number of individuals affected.	Technical Lead
3.3 Assess Likelihood of Serious Harm	Evaluate the risk using factors like: the type of information, the duration of the exposure, and whether the information is protected (e.g., encrypted). *Serious harm includes physical, financial, emotional, or reputational damage.*	Response Leader
3.4 Document Findings	Keep a comprehensive log of all evidence, findings, and decisions made during the assessment phase.	All Team Members

4. Stage 3: Notification (Mandatory Reporting)

Notification is mandatory if the breach is deemed **likely to result in serious harm** to affected individuals (Notifiable Data Breach).

a. Notification to Individuals

If notification is required:

- **Content:** The notification must include a description of the breach, the kinds of information involved, and recommendations on steps individuals can take (e.g., change passwords, monitor accounts).
- **Method:** Notify affected individuals directly (e.g., via letter, phone, or email—but not via the compromised channel).
- **Timing:** Notification must be provided **as soon as practicable** after the breach is confirmed.

b. Notification to the Regulator (OAIC)

- The Club must lodge a statement about the eligible data breach with the **Office of the Australian Information Commissioner (OAIC)** via their online portal.

c. Notification Decision (If Not Serious Harm)

- If the Club determines the breach is **not** likely to cause serious harm, the decision and rationale must be documented and filed, even though mandatory notification is not required.

5. Stage 4: Review (Prevent Recurrence)

The goal is to learn from the incident and improve security.

Step	Action	Responsibility
5.1 Post-Incident Review	Conduct a full review of how the breach occurred, how the response was executed, and what gaps led to the incident.	Response Leader
5.2 Implement Remediation	Implement technical and procedural changes identified in the review (e.g., purchase better firewall software, mandate MFA, update this policy).	Technical Lead / Committee
5.3 Staff Training	Conduct refresher training for all volunteers and staff on the specific security weakness that led to the breach.	Response Leader
5.4 Policy Update	Update this Data Breach Response Plan and the wider IT Policy to reflect lessons learned.	Response Leader