WyndhamRC

DATA GOVERNANCE FRAMEWORK

Data Governance Policy | Website Privacy Policy | Data Register & Retention Schedule

Document owner	WyndhamRC Committee	**Version**	1.0
Responsible officer	Secretary / Privacy Officer	**Status**	For Committee Adoption
Approval date	[insert date]	**Review cycle**	Annual
Next review	[insert date]	**Classification**	Committee Controlled / Public sections identified

Committee resolution

Proposed resolution: That the WyndhamRC Committee adopts the WyndhamRC Data Governance Framework Version 1.0, authorises the Secretary/Privacy Officer to implement it, and requires an annual review of access, retention and third-party services.

1. Data Governance Policy

Purpose

WyndhamRC will collect, use, store, disclose and dispose of personal information responsibly, securely and only where reasonably required for club activities. The Australian Privacy Principles (APPs) are adopted as a governance benchmark where practicable, whether or not every APP is legally binding on the Club.

Governance principles

- Collect only information reasonably necessary for a stated purpose and explain that purpose at or before collection.
- Minimise collection of sensitive information and information about children; obtain parent/guardian involvement where appropriate.
- Use approved systems and reputable service providers; apply Multi-Factor Authentication (MFA) wherever available.
- Restrict access by role and need-to-know; promptly remove access when a role ends.
- Do not circulate sensitive form contents in routine notification emails; direct authorised officers to the controlled system.
- Retain information only for the approved period, then securely delete or de-identify it unless law, insurance or governance requirements justify longer retention.

Information classification

Class	Examples	Control
General	Non-personal website content	Normal website controls
Personal	Name, email, phone, address, membership information	Approved system, restricted access, MFA
Sensitive / Restricted	Health/accessibility, emergency details, child information, identity documents	Need-to-know access; enhanced protection; collect only when justified

Policy controls and responsibilities

Approved systems: Netlify Forms for low-risk website enquiries; Jotform for structured applications/registrations requiring stronger form controls; Google Workspace/Drive/Sheets for approved administrative and longer-term records.

Personal devices: Personal cloud storage, uncontrolled spreadsheets and other unapproved repositories must not be used for Club personal information unless specifically authorised.

Access: Use individual accounts where available. Shared passwords are prohibited where individual accounts can be used. Review permissions at least annually and whenever office holders or volunteers change.

Email: Prefer notification-only messages. Sensitive/Restricted data should remain in the controlled system rather than being reproduced in email.

Data breach: Any suspected loss, unauthorised access/disclosure, account compromise or other breach must be reported immediately to the President, Secretary or Privacy Officer. Response: Contain -> Assess -> Record -> Notify where required -> Remediate.

2. Public Website Privacy Policy

Public document - publish on the WyndhamRC website and link from every form.

Information we collect

Depending on the form or service, WyndhamRC may collect a name, email address, telephone number, enquiry/message details, membership or program information, parent/guardian information where appropriate, and other information voluntarily provided. We aim to collect only information reasonably required for the requested service.

Why we collect it

Information may be used to respond to enquiries, administer membership, training, events and club activities, communicate with participants or guardians, maintain appropriate records, and meet safety, insurance, governance or legal requirements. WyndhamRC will not sell personal information.

Storage and service providers

WyndhamRC may use reputable third-party providers including Netlify, Jotform and Google to collect, process or store information. Information may be stored or processed outside Australia depending on the provider, service and account configuration. WyndhamRC applies reasonable administrative and technical safeguards and limits access to authorised persons.

Sensitive information and young people

Sensitive information will only be requested where reasonably necessary for a club activity, safety requirement or other legitimate purpose. Information concerning children or young people will be minimised and a parent or guardian involved where appropriate.

Retention

Personal information is not intended to be retained indefinitely. WyndhamRC applies its Data Register & Retention Schedule and deletes or de-identifies information when no longer reasonably required, subject to legal, insurance, safety and governance requirements.

Access, correction and concerns

A person may contact WyndhamRC to ask what personal information is held about them, request correction, raise a privacy concern, or request deletion where appropriate. Privacy contact: Secretary, WyndhamRC - [insert official email].

Recommended form collection notice

> *"WyndhamRC uses the information you provide to respond to this enquiry or administer the requested service. Please see our Privacy Policy for information about use, storage, access and deletion."*

3. Data Register & Retention Schedule

The periods below are WyndhamRC governance settings. Where legislation, insurance, a court/tribunal order or another binding requirement requires longer retention, that requirement prevails.

Information	System	Class	Access	Retention
General website enquiry	Netlify	Personal	Secretary / web admin	6 months after resolved
Come & Try enquiry	Netlify	Personal	Secretary / coordinator	6 months after activity/enquiry
Flight Academy initial enquiry	Netlify	Personal	Secretary / authorised instructors	6 months after resolved or transferred
Spam / unsolicited forms	Netlify	Low	Web administrator	Delete promptly
Formal membership application	Jotform	Personal	Secretary / membership officer	Transfer to approved member record; delete form within 3 months
Junior registration	Jotform	Restricted	Secretary / authorised program officer	Participation + 12 months, unless longer justified
Parent/guardian contact	Jotform / Google	Personal	Authorised program officers	Participation + 12 months
Emergency contact	Jotform / Google	Restricted	Authorised officers/instructors	Delete/update when participation ends; max 12 months thereafter
Health/accessibility information	Jotform / secure store	Sensitive	Demonstrated need only	Review annually; delete when no longer required
Member master record	Google Workspace	Personal	Secretary / membership officer	Membership + 7 years, subject to legal/insurance review
Membership payment/accounting	Google / accounting	Financial	Treasurer / authorised officers	7 years
Committee governance records	Google Workspace	Governance	Authorised Committee	Permanent or governance schedule
Incident/accident record	Google / secure store	Restricted	President / Secretary / Safety Officer	7 years minimum; longer if required
Website analytics	Netlify / approved analytics	Technical	Web administrator	12 months where configurable
Form notification email	Google/Gmail	Personal	Intended authorised recipient	Delete after actioned; target 90 days
Exported CSV/Excel forms	Temporary approved storage	Personal/Restricted	Authorised officer	Delete immediately after approved transfer/processing

Platform operating rules

Netlify - Treat as the website front door, not the permanent personal-information archive. Collect minimum necessary data; review and delete submissions to schedule; do not ordinarily collect Sensitive/Restricted data in general enquiry forms.

Jotform - Use for structured applications/registrations where stronger controls are appropriate. Enable MFA and appropriate encryption/security options. Delete source submissions after approved transfer and the scheduled retention period.

Google - Use as the controlled administrative record environment. Apply role-based access and MFA; prohibit unrestricted sharing links; review permissions annually and whenever roles change.

Implementation & Annual Compliance Checklist

Implementation actions

#	Action	Required control	Complete / date
1	Committee adoption	Approve this Framework by recorded resolution and nominate the Secretary or another officer as Privacy Officer.	☐
2	Form inventory	List every WyndhamRC website/application form and map each field to a documented purpose.	☐
3	Data minimisation	Remove fields that are not reasonably required; separate initial enquiry data from formal membership/sensitive data.	☐
4	Account security	Enable MFA on Netlify, Jotform and Google accounts where available; eliminate shared passwords where individual accounts are supported.	☐
5	Permissions	Limit access to role and need-to-know; remove former office holders, instructors and volunteers promptly.	☐
6	Email controls	Configure notification emails to avoid reproducing sensitive form contents wherever practicable.	☐
7	Retention	Set calendar/administrative reviews for Netlify, Jotform, Google and email against the schedule in this document.	☐
8	Website publication	Publish the Website Privacy Policy and place the collection notice adjacent to relevant form submission controls.	☐
9	Breach readiness	Keep a simple breach register and current contact pathway for President, Secretary/Privacy Officer and relevant providers.	☐
10	Annual review	Record the annual review outcome, access changes, expired records destroyed/de-identified, provider changes and policy amendments.	☐

Annual assurance questions

- ☐ What personal information does WyndhamRC currently hold, where is it stored and why is it still required?
- ☐ Are all authorised users current, individually identified and protected by MFA where available?
- ☐ Have expired Netlify/Jotform submissions, temporary exports and notification emails been deleted?
- ☐ Have service-provider terms, storage locations or security configurations materially changed?
- ☐ Have any data incidents, complaints or access/correction requests occurred and been documented?
- ☐ Do any retention periods need to be extended because of law, insurance, litigation, safeguarding or another documented requirement?

Governance basis

This Framework uses the OAIC's APP 11 information-lifecycle approach as a governance benchmark: reasonable technical and organisational measures should protect personal information from misuse, loss and unauthorised access, and information no longer needed should be destroyed or de-identified unless an exception applies. Victorian incorporated associations must retain financial records for seven years.

Committee adoption

President	_____	**Date**	_____
Secretary	_____	**Date**	_____