YMCA Geelong - Privacy Policy

OFFICE USE ONLY

Policy Number	Date Approved	Date Last Amended	Status
YG-126-G	Board approval pending 24/08/2026	30/06/2026	**DRAFT FOR REVIEW**

1. INTRODUCTION

Y Geelong is committed to fostering a respectful and safe workplace for all individuals involved in our organisation. To support this commitment, we have established a Policy Framework that applies exclusively to Y Geelong (Young Men's Christian Association of Geelong) and Geelong and District YMCA Youth Services, collectively referred to as 'The Y,' 'we,' 'us,' or 'our organisation.'.

The purpose of the policy is to ensure the Y meets legal requirements, ensuring it aligns with both strategic objectives and compliance standards. It also provides guidance on how Y People should respond if they witness or experience breaches of these standards.

The Policy Y Geelong recognises the importance of safeguarding personal information and is committed to handling all information with care, transparency and integrity. We value the trust placed in us by individuals, staff, volunteers, clients, we take our responsibilities as both an employer and a national body seriously when managing personal information throughout a person's engagement with us.

When we collect personal information, we aim to ensure you understand why it is being collected, how it will be used, and who it may be shared with via access to the YG 126-G Privacy Policy on online and on site.

Y Geelong complies with the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth). These principles guide the way we collect, store, use and disclose personal information across our organisation.
For more information about privacy rights and the Australian Privacy Principles, visit the Office of the Australian Information Commissioner (OAIC)

2. PRIVACY POLICY STATEMENT

At the Y we are dedicated to foster a culture of integrity, respect around how Y Geelong collects, uses, stores and protects personal information. It applies to anyone who interacts with us, including staff, volunteers, clients, young people, Member Associations, National Entities, contractors, partners and the public. This includes personal information collected through employment, recruitment, volunteering and contractor activities, as well as information collected when engaging directly with participants. The purpose of this Policy is to outline:

- What personal information we collect and hold;
- How and why we use and share it;
- How we protect it; and
- How you can access or correct your information or raise a concern.

Our approach to privacy reflects our commitment to care, respect and transparency in everything we do.

3. SCOPE

This policy applies to YMCA Geelong Inc., its Board, employees, managers, volunteers, contractors, agency workers, students, coaches, program leaders, affiliated clubs and any person or organisation that handles information on behalf of Y Geelong.

It applies to information handled in any format, including paper records, electronic systems, email, SMS, forms, images, CCTV, video, audio, online platforms, databases, cloud services, mobile devices, spreadsheets, shared drives, incident systems and archived records.

4. WHAT INFORMATION WE COLLECT

4.1 Personal information

Personal information is information or an opinion about an identified person, or a person who is reasonably identifiable. This may include name, address, phone number, email, date of birth, gender, emergency contacts, parent or guardian details, booking details, participation records, employment records, incident records, images, video, complaints and communications.

4.2 Sensitive and health information

Sensitive and health information may include medical conditions, disability, medication plans, allergies, injury information, behaviour support plans, risk assessments, cultural or language information, religious or dietary information, concession card details, custody or court order information, criminal history or screening information, child safety information and other information required to provide safe services.

4.3 Payment and financial information

YMCA Geelong may collect payment details, direct debit authorities, transaction records, bank account information, payroll details, superannuation details, tax file number information and funding or subsidy information. Credit card information must be processed securely and must not be stored unless authorised by an approved, secure and compliant payment system.

4.4 Children and young people

YMCA Geelong collects information about children and young people only where it is reasonably necessary to provide services, protect safety and wellbeing, comply with law, manage enrolments, communicate with parents or guardians, and meet regulatory obligations. Where appropriate, information will be collected from a parent, guardian or authorised representative; however, child safety and information sharing laws may permit or require collection or disclosure without consent in specific circumstances.

5. HOW INFORMATION IS COLLECTED

YMCA Geelong collects information through enrolment, membership and booking forms; employment and volunteer processes; online forms; email; phone; in-person interactions; social media and website interactions; incident and complaint reports; training and compliance systems; payment systems; surveys; competitions; partner referrals; regulators; health providers; emergency services; and other authorised third parties.

Where practicable, information will be collected directly from the individual or their authorised representative. Where this is not practicable or where law permits otherwise, information may be collected from another organisation, regulator, information sharing entity, emergency service, parent or guardian, referrer, investigator, insurer, legal adviser or other relevant party.

From others

In some cases, we may collect information about you from other people or organisations. This may include:

- Your parent or guardian, if you are under 18;
- Referees, government agencies or qualification bodies, when you apply for a role;
- State Sporting Associations or National Sporting Organisations
- if your information relates to an insurance claim, safeguarding matter or
- Other organisations or professionals involved in a claim or incident, where it is necessary for us to fulfil our role or meet legal obligations.

Through digital and online interactions

We use technology to help us connect with our community and improve how we communicate. This includes:

- Social media platforms such as Facebook, Instagram and LinkedIn; and
- Online services like survey or website tools (for example, WordPress).

When you use these platforms, the service providers may also collect and process your personal information under their own privacy policies. We encourage you to review their privacy settings or contact us directly if you prefer to communicate privately.

Website and analytics data

When you visit our website or digital platforms, we collect basic analytics data to understand website traffic and engagement, improve our marketing activities and enhance user experience.
This may include general information about your browser, device, approximate location or demographics.

You can choose to disable cookies or adjust your browser settings, although this may affect some website functions.

Unsolicited Information

If we receive personal information that we did not request, we will determine whether it is reasonably necessary for our work or if we are legally permitted to keep it. If not, we will securely delete or de-identify the information as soon as practicable.

6. WHY INFORMATION IS USED AND DISCLOSED

YMCA Geelong uses and discloses information for the primary purpose for which it was collected and for related purposes that a person would reasonably expect, or where consent has been provided, or where required or authorised by law. Common purposes include:

- delivering programs, memberships, bookings, camps, sport and recreation, gymnastics, OSHC, holiday programs and community services;
- communicating with participants, families, staff, volunteers, contractors, schools, partners and visitors;
- supporting inclusion, accessibility, medical needs, behaviour support, supervision, safety planning and emergency response;
- administering employment, recruitment, onboarding, payroll, training, performance, rostering, wellbeing, workers compensation and volunteer management;
- reporting to regulators, government agencies, funders, insurers, auditors, affiliated sporting bodies, Y Australia, Y Safeguarding, ACECQA, the National Quality Agenda IT System, child safety agencies and law enforcement where required or permitted;
- handling complaints, incidents, allegations, reportable conduct, child safety matters, legal claims, investigations, quality assurance, risk management and insurance;

- processing payments, direct debits, refunds, concessions, subsidies and accounts;
- maintaining security, protecting systems, preventing fraud, auditing compliance and improving services;
- sending service updates and lawful communications, including opt-out or unsubscribe options where required.

7. CONSENT, NOTICE AND CHOICE

By applying for, booking, enrolling in, participating in, visiting, volunteering for or being employed by YMCA Geelong, individuals consent to the reasonable collection, use and disclosure of information for the purposes described in this policy, relevant collection notices and service-specific forms.

Consent may be express or implied. Consent is not required where collection, use or disclosure is required or authorised by law, is necessary to prevent or lessen a serious threat to life, health or safety, is necessary for child safety or wellbeing under applicable information sharing laws, or is otherwise permitted under the Privacy Act, Health Records Act or other legislation.

Individuals may choose not to provide some information. However, this may limit YMCA Geelong's ability to provide services, confirm eligibility, safely supervise participation, process employment, comply with law, respond to emergencies or meet regulatory requirements.

8. DATA MANAGEMENT PRINCIPLES

8.1 Data minimisation

Collect only what is reasonably necessary for the service, employment, safety, legal, regulatory or operational purpose. Avoid collecting information just because it may be useful later.

8.2 Privacy by design

Privacy risks must be considered when designing new programs, forms, systems, campaigns, technology, data reports, AI tools, integrations or supplier arrangements.

8.3 Data quality

Reasonable steps must be taken to ensure information is accurate, complete, up to date and relevant before it is used or disclosed. Customers and employees are expected to update details through approved systems.

8.4 Access controls

Access must be role-based and limited to people who need the information to perform authorised duties. Shared accounts must not be used. Multi-factor authentication must be used where available.

8.5 Secure storage

Information must be stored in approved secure systems, locked cabinets or controlled folders. Personal information must not be stored on personal devices, unapproved USBs, personal email accounts or unsupported cloud services.

8.6 Data retention and destruction

Information must be retained only for as long as required by law, contract, safeguarding, insurance, governance or operational need. Records must be securely destroyed or de-identified when no longer required unless a legal hold applies.

8.7 Supplier and system governance

Third-party systems and contractors must be assessed for privacy, cyber security, confidentiality, access controls, data location, retention, breach notification and contract obligations before use.

8.8 Data sharing records

Material disclosures, information sharing requests, child safety information sharing and regulator disclosures must be recorded with the reason, authority, date, recipient and information disclosed.

8.9 Staff training

Employees, volunteers and contractors who handle personal information must complete induction and refresher training relevant to their role, including privacy, cyber security, records, child safety and incident reporting obligations.

9. SECURITY OF PERSONAL INFORMATION

YMCA Geelong will take reasonable steps to protect information from misuse, interference, loss, unauthorised access, modification and disclosure. Security controls may include password protection, multi-factor authentication, role-based permissions, secure hosting, device controls, encryption where available, audit logs, staff training, locked storage, supplier assurance and incident response procedures.

Employees, volunteers and contractors must immediately report suspected privacy incidents, cyber incidents, lost devices, misdirected emails, unauthorised access, phishing, accidental disclosure or missing records through the approved incident reporting process and to their manager or CEO delegate.

10. DATA BREACH RESPONSE AND NOTIFICATION

A data breach occurs when personal information is lost or accessed, disclosed, changed or used without authorisation. YMCA Geelong will contain the incident, assess the likely risk of serious harm, take remedial action, document decisions and notify affected individuals and the OAIC where the Notifiable Data Breaches scheme requires notification.

Where health information, child safety information, staff information, government identifiers, payment information or regulator-held information is involved, additional notifications may be required to relevant regulators, insurers, funders, service partners, police, IT providers, the Board or legal advisers. The CEO or delegated privacy lead will coordinate any external notification.

11. ACCESS, CORRECTION AND COMPLAINTS

Individuals may request access to, or correction of, their personal or health information by writing to the CEO or authorised privacy contact. YMCA Geelong will respond within 30 days where practicable unless a shorter timeframe is required by law. Access may be refused or limited where permitted by law, including where release would create a safety risk, breach another person’s privacy, prejudice an investigation, or disclose legally privileged or excluded information.

Health information corrections must be managed in accordance with the Health Records Act. Where information cannot be deleted, an amendment, statement or correction note may be attached to the record.

Privacy complaints must be handled under the YMCA Geelong complaints process and escalated to the CEO where required. If a person is not satisfied, they may contact the OAIC for Privacy Act matters, the Health Complaints Commissioner for health information matters, or OVIC where Victorian public sector privacy obligations or information sharing schemes apply.

12. OVERSEAS DISCLOSURE AND CLOUD SERVICES

YMCA Geelong will not disclose personal or health information overseas unless the individual consents, the disclosure is required or authorised by law, or appropriate privacy protections are in place. Some approved software, cloud hosting, support or data processing services may be located outside Australia or may be accessible by overseas support teams. YMCA Geelong will take reasonable steps to ensure those services protect information consistently with Australian privacy obligations.

13. AUTOMATED DECISIONS, AI AND ANALYTICS

YMCA Geelong may use digital systems, reporting tools, analytics or artificial intelligence to support administration, rostering, communications, compliance tracking, incident reporting, risk review and service improvement. YMCA Geelong will not rely solely on automated decisions for decisions that significantly affect an individual's rights, safety, employment or service access unless the process is lawful, transparent, reviewed by an authorised person and described in relevant notices where required.

Personal, sensitive, health or child safety information must not be entered into public AI tools or unapproved platforms. Approved AI or analytics tools must be assessed for privacy, security, data location, retention, confidentiality and human oversight.

14. CHILDREN, SAFEGUARDING AND INFORMATION SHARING

Child safety and wellbeing take priority in YMCA Geelong information handling. Information may be shared without consent where permitted or required to promote child wellbeing or safety, respond to allegations, manage reportable conduct, support mandatory reporting, assist an investigation, protect a child or group of children, or comply with the Child Information Sharing Scheme, Reportable Conduct Scheme, Education and Care Services National Law, Safeguarding requirements or other legal obligations.

Information sharing must be purposeful, proportionate, documented and limited to what is necessary. Employees must consider whether the information is excluded information, whether sharing may increase risk, and whether views of the child and family can safely and appropriately be considered.

15. MARKETING, MEDIA, PHOTOGRAPHY, CCTV AND DIGITAL COMMUNICATIONS

Direct Marketing
We may use your contact details to send you updates, newsletters or information about our programs and initiatives that we think may be of interest to you. You can opt out of receiving these communications at any time by following the unsubscribe instructions in our emails or by contacting us directly.

Use of Photos and Marketing Materials
We sometimes use images, videos or stories of individuals to promote our programs and share the positive impact of our work.
We only use this type of images and information with informed consent.

Sharing Information with Third Parties
When sharing information with third parties, we take steps to ensure that it is handled securely, used only for the purpose it was provided, and protected in accordance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles.

Photographs, video, audio and digital content that identify a person are personal information

YMCA Geelong will seek appropriate consent for promotional photography, publication and social media use unless another lawful basis applies. Images or recordings of children must be managed in accordance with child safety, devices, photography, social media and consent procedures.

CCTV or surveillance systems, where used, must be clearly notified, securely managed, accessed only by authorised people and retained only for an approved period unless needed for safety, investigation, legal or insurance purposes.

SMS, email and electronic communications must use approved systems and sender IDs, include clear identification of YMCA Geelong where required, and provide unsubscribe or preference options for marketing communications.

16. SPECIFIC OPERATIONAL REQUIREMENTS

16.1 Education and care worker information

From 27 February 2026, YMCA Geelong as an approved provider must record, maintain and update prescribed education and care worker information in the National Early Childhood Worker Register through the NQA IT System. This may include identity, contact information, role, employment dates, service approval number, employment type, probation status where applicable, qualifications, child protection and child safety training, first aid, anaphylaxis, asthma, WWCC/WWVP or teacher registration details and expiry dates.

16.2 Safeguarding concern information

Where a person is involved in or connected with a safeguarding concern, YMCA Geelong may retain, use and disclose relevant information to Y Australia, Y Safeguarding, investigators, assurance providers, regulators, police, insurers and legal advisers. This may continue beyond the end of employment, volunteering, membership or participation where necessary for safeguarding, legal, regulatory, insurance or recordkeeping purposes.

16.3 Payment information

Credit card and direct debit information must be processed through approved payment systems. Paper payment forms must be securely stored until processed and then securely destroyed unless retention is required. Card details must not be written in notebooks, emailed, photographed or saved in unapproved documents.

16.4 Website, cookies and online services

YMCA Geelong websites and online systems may collect information through forms, cookies, analytics, e-commerce, enquiries and user interactions. Online collection must be supported by a privacy notice and reasonable security controls such as encryption and secure payment processing.

16.5 How to contact us

You can contact us about anything in this Privacy Policy, including if you would like to:

- request access to, or correction of, the personal information we hold about you;
- ask a question or raise a concern about how we collect, use or protect personal information; or
- request more information about how we manage privacy at Y Australia.

You can contact us by:

Email: info@ygeelong.org.au
Mail: Privacy Officer, Y Geelong, 25-33 Riversdale Road, NEWTOWN Vic 3220

16.6 Policy Updates

This Policy may change from time to time and is available on our website.

17. ROLES AND RESPONSIBILITIES

Department / Area	Role / Responsibility
Board	Ensure suitable governance, resources and oversight for privacy, cyber security, data management, risk and compliance.
CEO / Policy Owner	Approve procedures, monitor compliance, respond to serious complaints and breaches, oversee regulator notifications and report material privacy risks to the Board.
Senior Leadership Team	Promote a culture of privacy, lawful information sharing, child safety and secure data management. Ensure systems, suppliers and staff practices meet this policy.
Managers / Coordinators / Team Leaders	Ensure collection notices, records, access controls, training, incident reporting and retention practices are followed in their area.
Employees, volunteers, contractors and students	Handle information only for authorised purposes, keep it secure, complete required training, report breaches immediately and comply with this policy and related procedures.
IT / System Administrators / Approved suppliers	Maintain secure systems, access controls, audit logs, backup processes, breach support, cyber security controls and supplier assurance documentation.

18. MONITORING, EVALUATION AND REVIEW

Compliance with this policy will be monitored through internal systems, incident reporting, supplier reviews, privacy impact assessments, data breach records, training completion, audit activities, complaints and Board reporting where required.

Privacy incidents, complaints and material breaches must be reported to the CEO and escalated to the Board where there is legal, regulatory, safeguarding, reputational, financial or operational risk. This policy will be reviewed at least every four years, or earlier if legislation, regulator guidance, systems, services or organisational risks change.

19. DEFINITIONS

Term	Meaning
Personal information	meaning any information or opinion about you that can identify you. This includes things like: • Your name, address, phone number, and email • Your date of birth and age • Your bank details or credit card information • For staff, contractors and volunteers, this includes information held for employment, payroll, performance and health and safety purposes.
Sensitive information	is a special type of personal information that is more private and needs extra protection. This includes things like: • Your health information (like medical history or disabilities) • Your racial or ethnic background • Your religious or philosophical beliefs • Your sexual orientation • Membership of a political party or trade union • Your criminal record
Health information	Information about a person's physical, mental or psychological health, disability, health services, wishes for future health services, genetic information or personal information collected in providing a health service.
Data breach	A loss of, unauthorised access to, unauthorised disclosure of, or unauthorised use or modification of personal information.
Eligible data breach	A data breach likely to result in serious harm where remedial action has not removed the likelihood of serious harm.
Safeguarding concern	Any concern, allegation, incident, conduct or risk relating to the safety, wellbeing or protection of a child, young person or vulnerable person.
Automated decision	A decision made or materially supported by technology, analytics, algorithms or AI using personal information.
De-identified information	Information that no longer identifies an individual and is not reasonably capable of re-identifying the individual.

20. SUPPORTING DOCUMENTS, LEGISLATION AND GUIDANCE

Law / requirement	What this means for YMCA Geelong
Privacy Act 1988 (Cth) and Australian Privacy Principles	Sets requirements for open and transparent privacy management; collection notices; use and disclosure; direct marketing; cross-border disclosure; identifiers; data quality; security; access and correction.
Privacy and Other Legislation Amendment Act 2024 (Cth)	Introduces strengthened privacy reforms including children's online privacy code development, stronger OAIC enforcement powers, security and retention reforms, cross-border mechanisms, automated decision transparency requirements, statutory tort for serious invasions of privacy and doxxing offences.
Privacy Regulations 2025 (Cth)	Supports the Privacy Act, including prescribed exceptions and operational rules relevant to APP obligations, government identifiers and specified information handling activities.
Notifiable Data Breaches scheme - Part IIIC Privacy Act	Requires assessment and notification to affected individuals and the OAIC where an eligible data breach is likely to result in serious harm.
Health Records Act 2001 (Vic) and Health Privacy Principles	Applies to health information held by private and public sector organisations in Victoria, including medical conditions, disability, medication, injury, incident and health service information.
Privacy and Data Protection Act 2014 (Vic)	Relevant when YMCA Geelong acts as a contracted service provider or information sharing entity, and for Victorian privacy principles and protective data security expectations.
Child Wellbeing and Safety Act 2005 (Vic), including Child Safe Standards, Reportable Conduct Scheme, Child Information Sharing Scheme and Child Link where applicable	Permits or requires information sharing to promote child wellbeing and safety, supports safeguarding responses, and requires accurate records of child safety decisions and disclosures.
Children, Youth and Families Act 2005 (Vic)	Supports mandatory reporting and child protection information handling where child safety concerns arise.
Education and Care Services National Law Act 2010 and Education and Care Services National Regulations 2011	Applies to OSHC and education and care services, including enrolment records, incident records, child safety reforms and regulatory reporting.

National Early Childhood Worker Register requirements	Requires approved providers to record, maintain and update prescribed worker information in the NQA IT System from 27 February 2026, including identity, contact, role, employment, qualifications, training and WWCC/teacher registration details.
Worker Screening Act 2020 (Vic)	Supports Working with Children Check and worker screening information handling for employees, volunteers and contractors.
Fair Work Act 2009, Superannuation Industry (Supervision) Act 1993, Taxation Administration Act 1953 and tax file number rules	Allows collection and use of employee and contractor information for lawful employment, payroll, tax, superannuation and workforce management purposes.
Spam Act 2003, Do Not Call Register Act 2006 and SMS Sender ID Register requirements	Supports compliant electronic marketing, customer messaging, sender identification and unsubscribe practices.
Charter of Human Rights and Responsibilities Act 2006 (Vic)	Requires privacy, equality, cultural safety and human rights considerations in Victorian service delivery contexts.
Associations Incorporation Reform Act 2012 (Vic), ACNC obligations, insurance and funding agreements	Requires appropriate organisational, governance, financial and reporting records to be retained and protected.

Approved by: YMCA Geelong Board

Meeting number and date: Board approval pending

Effective date: Board approval pending 26/08/2026

Review date: 30/06/2030

Policy Owner: CEO

Contact details policy owner: Ph: 5223 2714 E: info@ygeelong.org.au

Amendment history:

Version	Date	Author	Change Description
V1	11/02/2014	Shona Eland	Uploaded to YMCA Geelong policy template; included scope, monitoring and evaluation clauses.
V2	27/05/2014	Shona Eland	Updated clauses to reference Privacy Amendment (Enhancing Privacy Protection) Act 2012 changes to the Privacy Act 1988.
V3	20/03/2017	Rebecca Johnson	Added notification of data breaches and supporting documents reference.
V4	07/05/2018	Shona Eland	Added YG 183-O Document Development, Archiving, Destruction and Access Policy.
V5	07/03/2019	Brenda Bowell	Updated review date.
V6	26/05/2020	Shona Eland	Inserted COVID-19 personal data collection requirement.
V7	27/01/2026	Shona Eland	Updated employee information accuracy, employee portals, transferred data flows and ACECQA worker information transfer requirements.
V8	30/0826/2026	Shona Eland	Reviewed and condensed policy into plain English and updated content for Privacy Act/APPs, Privacy and Other Legislation Amendment Act 2024, Privacy Regulations 2025, Health Records Act, Privacy and Data Protection Act, Child Information Sharing Scheme, National Early Childhood Worker Register, data governance, AI/automated decisions, cloud services, breach response and retention. Policy name changed to Privacy and Data Management Policy.

As adopted by the YMCA of Geelong on / / 2026

Shona Eland

Chief Executive Officer, YMCA Geelong Inc.