OAC Privacy Policy (including Grievance Procedure and Code of Conduct)

Version 2.0
Approved August 2018

1. APPLICATION OF THE PRIVACY PRINCIPLES

1.1. The Australian Privacy Principles (APPs) derives from the *Privacy Act* and applies from 12 March 2014
1.2. OAC Ministries is considered an APP entity and an 'organisation' for the purposes of the Privacy Act
1.3. As an organisation, we deal with 'Personal Information' and 'Sensitive Information' as defined by the Privacy Act
1.4. Exemptions provided by the Privacy Act which apply to OAC Ministries operations include;
- Current and former employee records
- Permitted general use (*Privacy Act s16A*). This is specifically relevant to Child Protection requirements which can include a wide range of record keeping
- Permitted health information (*Privacy Act s16B*)

1.5. This policy and related procedures may be updated upon changes to legislation, internal reviews or major privacy incidents

2. INFORMATION HELD & PURPOSE OF HOLDING

The following table provides details as to what information we will hold and the primary purposes for which it is held:

INFORMATION HELD	PURPOSE OF HOLDING
2.1 Individuals or organisations who support or have interest in OAC Ministries, and individuals who purchase OAC resources:	
Personal details *(names, address, email, telephone number etc.)*	• Maintaining database for direct contact • Mailing lists for newsletters, prayer lists and other communications • Sending receipts or invoices
Financial details and records of donations and donators	• Receipting of donations • Regular repeated donations • Accounting and auditing requirements
Record of purchases	• Receipting and invoicing • Accounting and auditing requirements
2.2 Employee, committee members and volunteer records:	
Personal contact details	• Maintaining legally required records • Maintaining database for direct contact
Permitted health information	• As required for events in the case of medical emergencies and incidents • Dietary requirements when food is provided as part of an event
Permitted employee records *(financial details, government identifiers etc)*	• Maintaining legally required records • Accounting and auditing requirements
Screening and training records *(background checks, interview records, training attendance and test results, event attendance etc)*	• Maintaining legally required records • Screening individuals to ensure suitability and safety • Recording history of volunteer involvement
Reference checks	• Screening individuals to ensure suitability and safety

Conflict resolutions, discipline processes, internal investigation details	• To internally pursue issue solution • Internal review of potential issues • Records required for potential legal purposes
Sensitive information including personal beliefs, criminal records etc.	• Screening of individuals to ensure suitability to the vision, mission and beliefs of OAC • Child protection and risk mitigation
Note: Employee record exemptions apply only to employees of OAC. Exemptions may also apply to volunteer records regarding safety or other legal requirements (e.g. child protection records)	

2.3 Individuals counselled or advised:

Personal contact details	• For further contact as appropriate for the counselling/advice involved
Details of matters discussed which may be referred to in later discussions	• For further counselling and advice • For clarity should a safety concern arise

2.4 Program or event participants:

Personal contact details	• Maintained for legally required records • Contacting guardians in the event of an incident
Permitted health information	• Providing details in a medical emergency
Records of event attendance	• Event attendance numbers • Maintaining records of individuals event attendance
Note: This applies to information provided by guardians for minors attending programs or events.	

2.5 Other organisations or individuals with whom we have contact regarding our products, services or general operations:

Contact details	• Responding and contacting regarding product or services • Maintaining and responding to complaints
Inquiry details	• Internal follow-up of inquiries • Internal investigations and records of complaints

3. INFORMATION COLLECTION

Any personal or sensitive information may be collected in the following ways:

3.1. From current or prospective employees, volunteers, committee members;
- Online or written registrations and forms
- Indirectly collected through reference checks (with the individual's assent)
- Interviews and discussions
- Criminal, Police or working with children type checks (with the individual's knowledge)
- Training and tests for screening and suitability
- Incidents reports and investigations
- Meeting minutes, attendance etc.
- Communications as part of authorised work

3.2. From event attendees or program participants (including guardians on behalf of minors);
- Online or written registration and forms
- Inquiries regarding events or programs
- Incident reports and investigations
- Record of event attendance or program attendance
- Follow up correspondence
- Providing payment information

3.3. From supporters or interested individuals;
- Online, written or verbal subscription to mailing lists
- Online, written or verbal request for individual or specific information and communication
- Online, written or verbal payment or payment details as donation
- Through conversation with an OACM worker or representative

3.4. From customers, businesses or other organisations;

- Inquiries or requests for products or services
- Professional communications
- Providing payment information

3.5. From those counselled, advised or discipled by an OAC worker;

- Interviews and discussions

4. STORAGE

How information is held and accessed:

4.1. Information is held by OAC Ministries in any of the following ways:

- Digital data stored locally at OAC facilities and on OAC computers/servers
- Data stored on organisation managed databases
- Data stored on secure, organisation managed cloud services
- Physical data stored in secured locations within OAC facilities
- Physical and digital information held temporarily by OAC workers

4.2. How and where information is held is based upon a combination of accessibility for the information's purpose, extent of storage security, sensitivity of the information, and any legal requirements for record keeping

4.3. Reasonable steps and restrictions will be used to ensure information is not misused, interfered with, lost, modified or disclosed outside of permitted purposes. Access to information may be granted to:

- Staff and authorised volunteers whose work is directly related to the purpose for which the information is collected outlined in this policy
- Administrative staff involved in the initial collection, storage, use or disclosure of information
- Special access by a staff member or authorised individuals to fulfil any functions outlined in this policy (e.g. disclosing information for legal reasons, updating information etc)

4.4. Staff, volunteers and any other workers who access information internally must follow our ***Privacy Code of Conduct (attached)***

5. USE & DISCLOSURE

How information is used and disclosed

5.1. Information may be collected and used for the primary purposes for which it is collected. Information will not be used for any other purpose unless:

5.1.1 the individual has consented to another use or disclosure; or

5.1.2 the individual would reasonably expect the information may be used or disclosed for a secondary purpose when:

- personal information is used for a secondary purpose related to the primary purpose; or
- sensitive information is used for a secondary purpose directly related to the primary purpose

5.1.3 there is a legal requirement or other permitted general situations and permitted health situations exemption for the use and/or disclosure of information or OAC Ministries believes using or disclosing the information is necessary for an enforcement body

5.2. When information is disclosed we will:

- Take reasonable steps to deidentify any information where possible in accordance with the purpose of the information
- Take reasonable steps to ensure the entity to which we are disclosing has policies and procedures which meet the APP

5.3. We will never:

- Sell personal or sensitive information
- Disclose information to entities outside of Australia (expect where required by law)

6. INFORMATION CORRECTION & DISPOSAL

6.1. We will attempt to correct any personal information if we have reason to believe that the information is inaccurate and correcting the information is aligned with the purpose for which the information is held

6.2. Where personal information is no longer required for its purpose by OAC and there is no legal requirement to retain information, the information will be securely destroyed and/or de-identified

7. REQUESTING ACCESS & CORRECTION

7.1. Upon request by an individual, OAC Ministries will give access to, or take steps to correct, information about the individual except where OAC is permitted to deny or limit access according to the *Privacy Act (APP 12.3 & 12.5)*

- If a request for access or correction is denied, we will provide a reason for denying the request in accordance with the APP, and the procedure to make a complaint about the refusal

7.2. Access or correction may be requested by phone or in writing via the National Office (contact details available at the end of this policy)

7.3. An individual does not need to provide a reason for a request to access information

7.4. If the request is granted, we will provide a reasonable range of choices as to how the individual may access the requested information

7.5. We will not charge a fee for lodging a request, for providing the information, or for correcting information

7.6. Responses to requests will be made within a reasonable period of time

8. GRIEVANCE PROCEDURE

8.1. Complaints or concerns regarding our handling or usage of information will follow our ***Privacy Grievance Procedure (attached)***

9. CONTACT

OAC Ministries - National Office

PO Box 4499, Doncaster Heights, VIC 3109

Email: national@oac.org.au

Phone: 03 9840

PRIVACY GRIEVANCE PROCEDURE

1. Any individual may make a complaint alleging: a breach of an individual's privacy, the mishandling of personal information, the refusal to give access to information, or a breach of the Australian Privacy Principles (APP).
2. Complaints may be made to us or directly to the Australian Information Commissioner
    a. Complaints to the Commissioner will, in most circumstances, be referred to us to enable us to attempt to first resolve the complaint.
3. When we receive a complaint, we will acknowledge receipt to the individual within 7 days of receipt.
4. We will ensure that we have sufficient detail to understand and investigate the complaint and if necessary, we will ask the individual to provide further explanation or material.
5. Within 14 days of receiving material sufficient to understand and investigate the complaint, we will inform the individual that we are investigating the complaint and will contact the individual again within 14 days.
6. During that time, we will prepare an Investigation Report (the 'Report') which, due to the nature of the material, will be kept confidential and accessed only in accordance with our Privacy Policy and the Privacy Act 1988 *(as amended).*
7. Once the Report is prepared, the individual will be invited to discuss the complaint with us with a view to resolution of the complaint.
8. The individual will have access to the contents of the Report in accordance with our Privacy Policy and the Privacy Act 1988 *(as amended).*
9. If we are able to resolve the matter, the terms of the resolution should be recorded in writing, signed as agreed by us and the individual and, if required, provided to the Commissioner.
10. If:
    a. We, or the individual, decline to participate in a meeting or
    b. Resolution as a whole or in part is not achieved at the meeting
    c. Either we or the individual may propose a mediation of the dispute conducted by a mediator agreed between the parties or, in the event that there is no agreement, as nominated by the Commissioner.
11. If:
    a. We, or the individual, decline to participate in a mediation or
    b. Resolution as a whole or in part is not achieved at the mediation
    c. The matter can then be referred to the Information Commissioner for assistance.
12. To assist the Information Commissioner, we will provide:
    a. The Report provided we are satisfied that to do so will not breach our obligations under the Privacy Act 1988 *(as amended)* and
    b. Details of matters which remain in dispute and
    c. A further report detailing the steps taken to resolve the complaint prior to the Commissioner's involvement.

PRIVACY CODE OF CONDUCT

Employees, volunteers, and agents are expected to conduct work in a manner that complies with the expectations listed below:

1. Work within the guidelines outlined in the organisational Privacy Policy.
2. Do not gather personal information without obtaining the individuals consent (implied or explicit). This is particularly relevant when working with children as the parent's permission must be obtained when recording children's personal information.
3. If you collect personal information, inform the individual of the organisation's identity and contact details, the purpose for collecting the information and how the information will be used and disclosed. Also inform the individual of the consequences if they do not provide the requested information.
4. Do not access personal or sensitive information except where it is being used for its intended purpose and you are authorised to work with OACM for that purpose.
5. Make every effort to ensure that personal information you collect is accurate, complete and up to date before you use the information.
6. Ensure that personal information you collect is protected from misuse, loss or unauthorised access as per organisational procedure.
7. Offer individuals, where practical, the opportunity of not identifying themselves when providing services to individuals.
8. Only collect sensitive personal information where it is directly related to the provision of services to individuals or groups of people.
9. Staff should assess and maintain security of locations in which information is stored including:
    a. Secure locks on rooms, cupboards, filing cabinets containing physical information,
    b. Use appropriate and effective passwords and encryption where possible for digital data,
    c. The level of security should be determined by the sensitivity of the information and the necessary accessibility for the information's purpose.
10. Information should remain secure even when in an authorised individual's possession such as avoiding leaving it open and accessible, keeping it locked or in a secure location, keeping track of where the information is and why you have it in your possession. Any such information should be returned to OACM property or storage as soon as possible and all other copies appropriately deidentified and destroyed. Any data held on personal devices used for OACM work should be appropriately secured with passwords and, if possible, encrypted.