Seventh Day Adventist Reform Movement
Australian Union Conference

Privacy Policy

Approved Version 1 (2025.v1)

Introduction: Why Privacy Is Important

Our organisation needs to collect information to fulfil its mission to serve, protect and comply with government requirements. While the collection of personal information is required, we have a duty to protect personal information and use it responsibly. This privacy policy outlines why we collect information, what information we collect and how to access and use it responsibly.

Why We Collect Information

Areas where we collect and/or use information include ChurchSafe, Content Resource Management, Membership Rolls, Elections and Officers Lists, for Church Programs and Events and when administering/using IT Services. These areas have different needs and are outlined individually.

ChurchSafe Privacy Policy

We collect information about church workers and volunteers (members and non-members) as required by law and by our ChurchSafe Policy. This information may include but is not limited to: name, date of birth, Working With Children Check or Blue Card details and records, Police checks and other checks, training records and certificates, contact details (phone, email and address), Union, Conference, Field or Local Church Officers lists and election/employee records. If you choose not to share this information with us, it will limit how you can serve in our organisation.

We also collect information about members and non-members for the purpose of making our organisation and community a safer place. This may be collected directly from you or from a person sharing a concern. This information is generally of a confidential nature and disclosure is limited by our policies and requirements of law. Our policy, forms and procedures can be viewed in our ChurchSafe Manual at: https://my.sdarm.org.au/ChurchSafe

We keep your information for the purposes of ChurchSafe and the WWCC and/or Blue Card Register. We share the required information on a needs-to-know basis for the purposes of ChurchSafe, so that programs and positions can be filled by suitably qualified staff. We may also share it with the SDARM Australasian Union Conference and units under it, as requested, according to their guidelines and where required by law.

We require each staff member, both paid and unpaid, to abide by responsible data storage, access, use and sharing. Please store all personal information securely, only access information when you need to, use personal information responsibly and for the purpose it was collected, only share how much you need to and only when you need to share it. Seek guidance from leadership (Church, Field, Conference or Australasian Union Conference) where you have questions about the best practice with the storage, use or handling of ChurchSafe information.

Content Resource Management (mySDARM) and Membership Rolls

The Contact Resource Management System (CRM) has been implemented to help Church Ministry to contact and serve members and contacts, for Secretaries to maintain secretarial records and facilitate

transfers between units. The CRM also forms part of the Treasurers' records, event registrations/payments and ChurchSafe Records.

Disclosing Personal Information

The CRM system stores contact and subscription information for church members and contacts. This information is held in trust and is not to be made public.

Users are only to use the information in fulfilling their roles within the church organisation, in an official capacity. Users are not to access the information for personal use, or to disclose the information to any unauthorised person.

Sometimes a person may request the address or phone number of another person. We may have this information in our system, but that does not mean we have authority or permission to give it to anyone who may ask. Thought and care must be taken to evaluate these issues and only provide information where there is a legitimate and proper reason to do so. These reasons would include the activities of our own workers, staff and any volunteer officers in the course of carrying out their official duties.

Elections and Officers Lists

Some details from ChurchSafe and Membership records are required to be shared to leaders, ministers and nominating committees. These details shared to maintain safe ministry and are to be kept confidential.

Lists of elected officers including officer's names and positions are publicly shared so that all can know who to contact for the different departments.

Church Programs and Events

Information on attendees, including but not limited their special needs (dietary, medical, etc), accommodation, seating and contact details are needed to tailor programs to participants needs, to ensure safe programs and are to be collected, stored and used responsibly for the purpose that they were gathered.

IT Services

Employees, AUC Officers and Department Leaders have an O365 account that includes a SDARM email address and mailbox and Microsoft apps including OneDrive.

Email Use and Storage

Church email addresses and mailboxes enable employees and leaders to reach and keep in touch with others. It is provided for church related correspondence and collaboration purposes. It is understood that each employee may from time to time receive direct correspondence of a personal, sensitive or confidential nature. For this reason, the AUC believes it is in the best interest of both employees/leaders and the AUC to ensure that all mailboxes are maintained in a safe and secure environment.

All are advised to be mindful of the material they send and keep on the server. While the AUC does not monitor employee emails, it is a requirement that the email system will not be used for any purpose that would bring disrepute upon the cause of God or is of an inappropriate or illegal nature.

If employees and officers choose not to use the church email system or wish to forward incoming emails to a personal address, they are to remember that church related emails are only to be sent to an address that they have sole access to. Email administrators can assist with setting up an auto forward of emails.

Microsoft 365 – OneDrive and Apps

Microsoft Apps including but not limited to OneDrive, SharePoint and Teams are helpful tools for team work and sharing. It is important that all use these tools to store, access, use and share data in a

responsible manner. It is possible to include external users on groups and this is often used for department committees. Please ensure that external users have sole access to the email accounts that you share data with and add to the online teams and groups.

It is possible for an administrator(s) to access users OneDrive for Business folders and files on the AUC server, but the AUC policy requires the users consent for this to happen. Installing and using the office programs and OneDrive for Business are optional. However, users need to remember the implications and responsibilities involved in doing so.

Mobile Device Management (MDM)

Mobile Device Management is used to secure and manage mobile devices that are accessing services provided by an Exchange server, including Office 365. Users need to enrol their devices (opt in) to the management system. Once a device is enrolled, an administrator can manage features on those devices and remotely wipe or adjust them if deemed necessary. While this is a feature of Office 365, the AUC will not be implementing MDM. However, all users are to take due care of their mobile devices to ensure work related content of a confidential or sensitive nature is kept secure. All users should password lock their mobile devices as a minimum.

Mailbox Privacy Policy

The SDARM AUC acknowledges that each employee and department may be provided from time to time with an electronic mailbox facility (including Email, Calendar, and Contact address book services).

This facility is provided primarily for church related correspondence and collaboration purposes. It is understood that each employee may from time to time receive direct correspondence of a personal, sensitive or confidential nature. The AUC believes it is in the best interest of both employees and the AUC to ensure that all mailboxes are maintained in a safe and secure environment.

The setup, administration and removal of mailbox users shall be by an approved Email Services Administrator.

No Email Services Administrator, nor any other person, shall access the contents of an employee's mailbox without the employee's written consent. In any other case where access may be deemed necessary, this shall be permitted only with the prior written approval of the AUC Executive Committee. Any breach of this policy will constitute a serious abuse of trust and result in loss of Administrator responsibilities and disciplinary action as determined by the AUC Executive Committee.

Privacy Guidelines

We acknowledge and seek to uphold the Australian Privacy Principles under the Privacy Act 1988. These are summarised as follows:

1. Only collect information that is necessary.
   Make sure individuals know what personal information your organisation or agency collects and why. Consider whether each piece of information is necessary for any of the functions or activities of the organisation or agency and whether the information is required in the circumstances. It may be the case that in some circumstances you can carry out your activities without collecting personal information, allowing individuals to interact with your organisation anonymously.

2. Do not collect personal information about an individual just because you think that information may come in handy later.
   You should only collect information that is necessary at the time of collection, not information that may become necessary or useful at a later date. If the need arises later, collect the information then.

3. Tell people what you are going to do with the personal information you collect about them.
   You should let individuals know why you need to collect the information, how you plan to use it and if you intend disclosing it. You should provide details about how they can contact you and, if they want to, how they can gain access to their personal information.

4. Consider whether you should be using personal information for a particular purpose.
   Organisations often begin using personal information for a secondary purpose unrelated to the main purpose they collected the information. Unless you have consent from the individual concerned or authorisation under law, you should normally only use personal information if it is related to the purpose you collected it for and within the reasonable expectations of the individual.

5. Consider whether you need to disclose personal information.
   In some cases, organisations and agencies disclose personal information that they do not need to disclose or disclose information without thinking about whether the disclosure is authorised. Consider whether you can achieve your purpose without disclosing personal information. It is often best practice to seek consent from the individual concerned if you wish to disclose their personal information for a reason beyond the reason for which you collected it. The Privacy Act allows disclosures in some circumstances.

6. If people ask, give them access to the personal information you hold about them. Organisations and Australian and ACT Government agencies have a general duty to provide individuals with access to their personal information. You should be as open as possible by providing individuals with access to their own personal information in the form they request. If you wish to deny an individual access to personal information you should provide reasons, consistent with the Privacy Act, as soon as you can. Agencies should also be mindful of their obligations under the Freedom of Information Act 1988 (Cth) which also provides some grounds for denying access.

7. Keep personal information secure.
   It is important that you keep personal information safe and secure from unauthorised access, modification or disclosure and also against misuse and loss. The steps you should take should be proportionate to the sensitivity of the information you hold. Methods might include checking that all personal information has been removed from computers before you sell them, installing firewalls, cookie removers and anti-virus scanners on work IT systems, keeping hard copy files in properly secured cabinets, training staff in privacy procedures and allowing file access to staff on a 'need to know' basis only. You could also regularly monitor your information handling practices to ensure they are secure and consider the adequacy of existing security measures. Depending on the size of the organisation and the information it collects, you may wish to consider having an external privacy audit conducted.

8. Don't keep information you no longer need or are no longer required to retain.
   If you no longer need personal information and there is no law that compels you to retain the information, then destroy it. You should shred, pulp or destroy the paper on which the personal information is recorded, place the files in a security garbage bin and securely delete any electronic record or file from computer systems to ensure it cannot be retrieved.

9. Keep personal information accurate and up to date.
   Personal information can change. This is why you need to take reasonable steps to keep the personal information your organisation or agency holds current. If the personal information of someone changes amend your records to reflect those changes and make sure both hard copy and electronic files are updated. If you know that some personal information is likely to change regularly, then periodically go through the files to ensure the records are accurate and up to date.

10. Consider making someone in your organisation or agency responsible for privacy.
    This could be a designated person (often called a Privacy Contact Officer or Chief Privacy Officer)

who is aware of your organisation or agency's responsibilities under the Privacy Act and who is willing and able to handle complaints and enquiries about the personal information handling practices of your organisation or agency. The person may also be responsible for implementing a complaints handling process, staff training program and promoting Privacy Act compliance.

Further Information on Privacy

Further information on privacy can be found at: www.oaic.gov.au