

ScoutHealth is the Scouts Victoria system used to collect, store and manage the Member Information. It has two access points. The ScoutHealth Member Portal is where Members and Parents provide and update their own Member Information. The ScoutHealth Management Portal is where authorised users view and manage the Member Information of the Members they are responsible for, so that we can run safe activities and respond quickly when a Member needs care.

This Agreement sets out the rules that apply to every authorised user of the ScoutHealth Management Portal. It explains how that access must be used, secured and protected. Because the Management Portal gives authorised users ready access to a large amount of Member Information, everyone who uses it carries a high level of responsibility to keep that information safe.

This Agreement supports our obligations under the Privacy Act 1988 (Cth) and the Australian Privacy Principles, and the Health Records Act 2001 (Vic) and the Health Privacy Principles. It applies in addition to the Scouts Victoria Health Records Data Management Policy and the ScoutHealth Collection Notice. Defined terms used in this Agreement have the meaning given to them in Section 3 or, where not defined here, in the Scouts Victoria Privacy Policy 2026.

2. Who this Agreement applies to

This Agreement applies to every Authorised User granted access to the ScoutHealth Management Portal, regardless of role, seniority or how often they log in. Authorised Users may include Leaders, authorised Scouts Victoria staff, the State Leadership team, and System Administrators.

By logging into the Management Portal, an Authorised User agrees to be bound by this Agreement, the Scouts Victoria Health Records Data Management Policy, the ScoutHealth Collection Notice, the Scouts Victoria Privacy Policy 2026, and any other applicable Scouts Victoria policy in force from time to time.

3. Definitions

Adult Member a registered Member of Scouts Victoria aged 18 or over.

Youth Member a registered Member of Scouts Victoria under 18 years of age.

Member a Youth Member or an Adult Member registered with Scouts Victoria.

Parent a person who has parental responsibility for a child. This may include a biological parent or another person who has been granted parental responsibility by a court order.

ScoutHealth the Scouts Victoria system used to collect, store, manage, access and report on Member Health and related Personal Information, accessed at scouthealth.com.au and governed by the Health Records Data Management Policy.

Management Portal the ScoutHealth access point through which Authorised Users view and manage the Member Information of the Members within their area of responsibility.

Member Portal the ScoutHealth access point through which Members and Parents provide and update their own Member Information.

Authorised User a Member or staff member who has been granted access to the Management Portal for an approved Scouts Victoria purpose, limited to their current role.

Personal Information information or an opinion about an identified individual, or an individual who is reasonably identifiable, and includes Sensitive Information, as defined under the Privacy Act 1988 (Cth).

Sensitive Information includes Health Information and other sensitive information as defined in the Privacy Act 1988 (Cth), such as religion, gender, criminal record, and information about relevant court or family violence orders.

Health Information information about a person's health, disability, allergies, medical conditions, medication, dietary requirements, treatment needs, action plans, emergency medical details or other information relevant to their health, safety or care.

Member Information all Personal Information (including Health Information and other Sensitive Information) held in ScoutHealth.

Need to Know an Authorised User requires access to information to perform their approved role, support safe participation, manage a health or safety risk, respond to an incident, or meet a legal, child safety, governance or operational obligation.

4. Access to the Management Portal

Access to the Management Portal is granted on a least-privilege, Need To Know basis. It is limited to Member Information of the Members an Authorised User is responsible for through their current role. Access is scoped as follows:

- Leaders can access the Member Information of Members within their area of responsibility, depending on their role.
- Authorised Scouts Victoria staff and the State Leadership team can access Member Information where it is required for their role.
- System Administrators can access Member Information only where required to administer, support, maintain, secure or audit ScoutHealth.

In every case, access is limited to authenticated users with a secure, individual user account.

Access is not transferable between individuals or roles. Where an Authorised User holds more than one position, they must only use the level of access appropriate to the function they are currently performing. Access is reviewed and updated or removed when a role changes, when access is no longer required, when a user changes Group, Section, District or Region, when membership becomes inactive, or when an employment or volunteer engagement ends. If a Member's membership is listed

as inactive in Scouts Victoria's membership system, access to their Member Information through ScoutHealth is revoked as a security measure.

5. Conditions of authorised access

- Access must be linked to the Authorised User's own individual account. Authorised Users must never log in using another person's account or credentials.
- Login credentials, including passwords and multi-factor authentication devices, must not be shared, written down insecurely, or disclosed to any other person, including other Members.
- Multi-factor authentication is mandatory on all Management Portal accounts and must not be disabled, bypassed or circumvented.
- Authorised Users must log out of the Management Portal on shared or public devices immediately after use. Use of public devices should be avoided where at all possible.
- Authorised Users must comply with their digital security obligations as set out in Section 6 of this Agreement.
- Members are responsible for promptly notifying State Office of any change in an Authorised User's role that affects their Management Portal access.

6. Digital security obligations

Authorised Users are responsible for protecting the security of their Management Portal account and any device used to access it. This includes:

- using a strong, unique password that is not reused across other services;
- keeping multi-factor authentication active and secure at all times;
- locking or securing devices when unattended, and logging out of shared or public computers immediately after use;
- keeping devices used to access the Management Portal up to date with security patches and reputable antivirus or anti-malware protection;
- avoiding access over unsecured public Wi-Fi where possible;
- not installing or using unauthorised third-party tools, browser extensions, scrapers or integrations that connect to ScoutHealth;
- not uploading, copying or transmitting Member Information to a personal device, personal cloud service, removable media, unmanaged personal device, file-sharing service, messaging service or app, survey platform, mailing-list platform or generative AI tool; and
- reporting a lost or stolen device, or any suspected unauthorised access to their account, immediately to the Privacy Officer (privacy.officer@scoutsvictoria.com.au) in accordance with Section 11.

7. Acceptable use

Management Portal access may only be used for legitimate Scouting purposes directly connected to the health, safety and care of Members within the authorised user's area of responsibility. In particular, Authorised Users must:

- access, use and share Member Information only to the extent reasonably required to perform their role, on a Need to Know basis;
- keep information accurate and up to date where they are responsible for maintaining it.

Authorised Users must not use the Management Portal for personal, commercial, political or fundraising purposes, or for any purpose outside Scouts Victoria's stated functions and activities.

8. Handling Member Information

The Management Portal holds Member Information about children, young people and adults. All access to and use of this information must comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles, the Health Records Act 2001 (Vic), the Health Privacy Principles, the Scouts Victoria Privacy Policy 2026 and the Health Records Data Management Policy. The following principles guide all handling of Member Information:

- **Safety first** relevant Member Information must be available to authorised people when reasonably required to protect a Member's health, safety or wellbeing.
- **Minimum necessary access** Authorised Users must only access the information that is reasonably necessary for the performance of their current role, a specific and legitimate Scouts Victoria function or activity, and the particular task being performed, on a Need to Know basis.
- **Confidentiality** Member Information must not be accessed, disclosed, discussed, downloaded, printed or shared unless required for an approved Scouts Victoria purpose.
- **Accountability** access, updates, exports and administrative actions are logged where technically available and may be monitored or audited for privacy, security and governance purposes.

The fact that information is visible or technically accessible through an account does not mean the user is authorised to access, use, download or share it. Member Information must not be accessed for curiosity, convenience, general reference, personal interest, future possible use or any purpose unrelated to the user's current role.

8.1 Discretion and confidentiality

Member Information must be handled discreetly at all times. Member Information must not be discussed in front of, or in a way that can be seen or overheard by, people who do not need to know

it. Screens showing Member Information must be kept away from public view, and conversations about Member Information should take place privately.

8.2 Use, disclosure and verifying recipients

Member Information must not be used for a purpose other than the purpose for which it was collected, or disclosed to an unauthorised person, unless the use or disclosure has been properly authorised by Scouts Victoria, is reasonably necessary for an approved function or activity, or is otherwise required or permitted by law.

A person is not authorised to receive Member Information merely because they are a Member, Leader, Commissioner, employee, volunteer, committee member, parent, guardian or carer. Before sharing any Member Information, the Authorised User must take reasonable steps to verify:

- the identity of the intended recipient;
- the recipient's current role or relationship to Scouts Victoria;
- that the recipient requires the specific information for an approved purpose;
- that the recipient is authorised to receive that category and scope of information; and
- that only the minimum information necessary is being shared.

8.4 Information about Youth Members

A heightened duty of care is owed to children and young people. Member Information about a Youth Member must only be accessed, used or shared for its intended Scouting purpose, and must not be used in a way that may place the Youth Member at risk of embarrassment, discrimination, harassment, harm or unauthorised identification. Particular care must be taken with information about a Youth Member's health, disability, medication, family circumstances, emergency contacts or other sensitive matters.

8.5 Taking Member Information to activities, camps and events

Authorised Users will often need offline access to Member Information to run a safe activity, for example an action plan, medication details, allergies or emergency contacts taken to a camp, hike or event where there may be no reliable connection. This is a legitimate use, and the following applies:

- take only the information needed for the Members actually attending, and only the fields required to keep them safe;
- keep printed and electronic copies secure at all times and out of public view;
- share the information only with the other Leaders who need it to care for those Members during the activity;
- do not upload, copy or transmit it to any other platforms or devices, in accordance with Section 6; and
- securely destroy or delete all copies once the activity has finished and the information is no longer needed.

8.6 Downloads, exports, screenshots and printed copies

Any report, export, download, screenshot or printed copy of Member Information from the Management Portal must be treated as confidential. An authorised user who creates or removes any such copy must:

- only do so where reasonably necessary for an approved purpose connected to their current role;
- limit the copy to the minimum records and data fields necessary for that purpose;
- store it securely and keep it protected from public view and unauthorised access;
- only share it with verified and authorised recipients on a strictly Need to Know basis;
- ensure electronic files are protected by appropriate access controls and, where required, encryption or password protection;
- not upload, copy or transmit the information to any unauthorised platform, in accordance with Section 6;
- not create or maintain an independent or unofficial health or membership database;
- not retain the information merely for convenience, general reference or possible future use, consistent with Section 8;
- securely delete or destroy the information when the approved purpose ends or the information is no longer required; and
- immediately report any actual or suspected loss, unauthorised access, incorrect disclosure or misuse of the information.

The restrictions in Section 6 on unapproved platforms and devices apply to any such copy, unless its use is expressly authorised by Scouts Victoria.

8.7 Access and correction

Members and Parents can access and update their own Member Information at any time through the Member Portal. Other requests to access or correct Personal Information can be made using the Information Request and Correction Form, or in writing to the Privacy Officer at privacy.officer@scoutsvictoria.com.au.

An Authorised User must not use their access to informally provide another person with copies of, or access to, Personal Information. Any request to access or correct Personal Information must be managed through the formal access and correction process.

9. Prohibited conduct

Authorised Users must not:

- share, publish or post Member Information, including on social media or messaging platforms, outside authorised Scouting channels;

- use Member Information to bully, harass, discriminate against, or otherwise cause harm to any Member;
- access the Member Information of a Member they are not responsible for, or that they have no approved reason to view, as set out in Sections 4 and 8;
- circumvent, disable or interfere with security controls, audit logging or access restrictions, including the multi-factor authentication requirements in Section 5;
- introduce malware, viruses or any code intended to disrupt or compromise ScoutHealth; or
- use automated tools, third-party integrations or browser extensions to scrape, bulk-extract or mine data from ScoutHealth without written authorisation from State Office (see also Section 6).

10. Monitoring and audit

Scouts Victoria may log, monitor and audit Management Portal activity, including login activity and data access, to protect the security, integrity and proper use of the system and the Member Information it holds, consistent with the Scouts Victoria Data Breach Response Plan 2026. Access privileges are reviewed periodically, and unusual or unauthorised activity may be investigated and may result in access being suspended pending review.

11. Reporting incidents and breaches

Any actual or suspected data breach, unauthorised access, loss of a device with Management Portal access, or misuse of Member Information must be reported immediately to the Privacy Officer (privacy.officer@scoutsvictoria.com.au). Where directed by the Privacy Officer, an Authorised User should also:

- record and advise the Privacy Officer of the time and date the suspected breach was discovered, the type of information involved, and the cause and extent of the breach, so far as known;
- take any immediately available and safe steps to contain the breach, for example recalling an email or securing a misplaced document, without destroying evidence; and
- not attempt to investigate the breach themselves, delete records, or notify affected individuals or external parties, unless directed to do so by the Privacy Officer.

The Privacy Officer will assess the breach and, where required, escalate and respond in accordance with the Scouts Victoria Data Breach Response Plan 2026, including any assessment and notification obligations under the Notifiable Data Breaches scheme.

12. Consequences of breach

A breach of this Agreement may result in one or more of the following: suspension or removal of Management Portal access; investigation; referral for disciplinary action under applicable Scouts

Victoria policies and By-Laws; membership action; and, where the conduct is unlawful, for example an unauthorised disclosure of a child's health information, referral to the Office of the Australian Information Commissioner, the Health Complaints Commissioner, Victoria Police, or other relevant authority.

13. Questions, requests and complaints

Questions about this Agreement, and complaints about how Scouts Victoria manages Personal Information, can be directed to the Privacy Officer:

- **Mail:** 152 Forster Road, Mt Waverley, VIC 3149
- **Email:** privacy.officer@scoutsvictoria.com.au

If a complaint is not resolved, it may be escalated to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992) or, for health information, the Health Complaints Commissioner (hcc.vic.gov.au, 1300 582 113).

14. Acknowledgement

I confirm that I have read, understood and agree to comply with this ScoutHealth Management User Agreement. I understand that my access is granted on the basis of my current role, that it may be varied or revoked at any time, and that a breach of this Agreement may result in the consequences described in Section 12.