Scouts Victoria

Health Records Data Management Policy

This Policy sets out how Scouts Victoria manages personal, sensitive and health information collected, stored, accessed, used, disclosed, exported or retained through ScoutHealth.

The purpose of this Policy is to ensure that ScoutHealth information is managed in a way that:

- supports the health, safety and wellbeing of Members;
- enables safe planning and delivery of Scouting activities, camps, events and programs;
- allows relevant health information to be accessed by authorised people when needed for health, safety, first aid or emergency response;
- protects personal, sensitive and health information from misuse, interference, loss, unauthorised access, modification or disclosure;
- supports Scouts Victoria's privacy, health records, child safety, legal, insurance and governance obligations; and
- provides clear expectations for users who access or manage information through ScoutHealth.

Scope

This Policy applies to:

- ScoutHealth;
- all personal, sensitive and health information collected, stored, accessed, updated, exported, downloaded, printed or otherwise handled through ScoutHealth;
- all users of ScoutHealth, including members, Parent, employees, system administrators and authorised Scouts Victoria personnel;
- all reports, PDFs, downloads, exports, printed copies and backups generated from ScoutHealth; and
- all environments where ScoutHealth data is stored, processed, administered, supported or accessed.

This Policy does not apply to all Scouts Victoria corporate records. Broader organisational membership records, employment records, financial records, insurance records, complaints records and other non-Health records must be managed under the relevant Scouts Victoria policies and procedures.

Related Documents

This Policy should be read together with:

- Scouts Victoria Privacy Policy 2026;
- ScoutHealth Collection Notice;

- Scouts Victoria Data Breach Response Plan;
- Scouts Victoria Child Safeguarding Policy 2021;

Where there is inconsistency between this Policy and any other Scouts Victoria policy, , the Privacy Policy and Collection Notice should be reviewed and legal advice sought before operational changes are made.

Definitions

Defined terms used in this Policy have the meaning given to them in this Policy or, where not defined here, in the Scouts Victoria Privacy Policy 2026.

Authorised user means a person who has been granted access to ScoutHealth for an approved Scouts Victoria purpose.

Health information means 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 means a youth or adult registered member of Scouts Victoria.

Need to know means the user requires access to the information to perform their approved role, support safe participation, manage health or safety risks, respond to an incident, or meet a legal, child safety, governance or operational obligation.

Parent means *a person that 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.*

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, and includes Sensitive Information.

ScoutHealth means the Scouts Victoria system used to collect, store, manage, access and report on member health and related personal information.

Sensitive information includes Health Information and other sensitive information as defined in the Privacy Act.

Guiding Principles

Scouts Victoria will manage ScoutHealth data in accordance with the following principles.

Safety first

Relevant health information must be available to authorised people when reasonably required to protect the health, safety or wellbeing of a member.

Privacy by design
ScoutHealth must be designed, configured and operated in a way that supports privacy, confidentiality, appropriate access, secure handling and accountable use of information.

Minimum necessary collection
Scouts Victoria will only collect information through ScoutHealth where it is reasonably necessary for Scouting activities, health and safety, emergency response, legal obligations, child safety, governance, risk management or related operational purposes.

Minimum necessary access
Users must only access information they need to perform their approved role or respond to a health, safety, welfare or emergency.

Accuracy and currency
Members or Parent are responsible for providing accurate and current information. Scouts Victoria will provide reasonable ways for information to be reviewed, updated and corrected.

Confidentiality
Information in ScoutHealth must be handled confidentially and must not be accessed, disclosed, discussed, downloaded, printed or shared unless required for an approved Scouts Victoria purpose.

Accountability
Access, updates, exports, downloads and administrative actions should be logged where practical to support auditability, governance, security monitoring and investigation of incidents.

Information Collected Through ScoutHealth
The types of personal, sensitive and health information collected through ScoutHealth are described in the ScoutHealth Collection Notice.

ScoutHealth must not be used to collect information that is unrelated to the approved purpose of the system.

Collection of Information
Scouts Victoria collects information through ScoutHealth only where reasonably necessary for the purposes set out in the ScoutHealth Collection Notice and the Scouts Victoria Privacy Policy 2026.

Information should be collected directly from the member or Parent wherever practical.

Users must be provided with the ScoutHealth Collection Notice before submitting information through ScoutHealth. By creating an account and submitting information

through ScoutHealth, the user consents to Scouts Victoria collecting, using and disclosing the relevant personal and health information in accordance with the Collection Notice and Privacy Policy.

Where the Parent provides information on behalf of a Youth Member, they are responsible for ensuring they have the appropriate authority or consent to provide that information.

Use of Information
Information in ScoutHealth may only be used for approved Scouts Victoria purposes. The purposes for which information collected through ScoutHealth may and may not be used are set out in the Scouts Victoria Privacy Policy 2026.

Access to ScoutHealth Information

Access to ScoutHealth must be restricted to authenticated users with a secure user account.

Access must also be role-based and limited to the information the user reasonably needs to perform their approved role.

Access levels may include:

- the individual to whom the information relates.
- the Parent of a Youth Member.
- Leaders will have access to members within their area of responsibility, dependent on their role.
- authorised Scouts Victoria staff and State Leadership team where required for their role.
- System Administrators - only where required to administer, support, maintain, secure or audit ScoutHealth.

Access must be reviewed and updated or removed when:

- a user's role changes.
- a user no longer requires access.
- a member changes Group, Section, District or Region.
- membership becomes inactive.
- Parent no longer has authority to access the relevant members information.
- Employment or volunteering engagement ends.
- access is no longer appropriate for security, privacy, legal or child safety reasons.

If a member is listed as inactive in Scouts Victoria's membership system, their access, and the access of their Parent where applicable, must be revoked or suspended as a security measure unless there is an approved operational reason to retain limited access.

Child Safety, Health and Emergency Access
Where necessary to protect a member's health, safety or wellbeing, relevant health information may be accessed by the appropriate authorised user with responsibility for managing the situation.

This may include access to information about:

- allergies and adverse reactions.
- medical conditions.
- medication information.
- dietary requirements.
- disability or support needs.
- action plans or emergency response instructions.
- emergency contact details.
- other information reasonably required to manage the health or safety issue.

Health information must be handled discreetly and must not be disclosed to people who do not need to know.

Downloads, Exports, PDFs and Printed Records

Any report, PDF, download, export, screenshot or printed copy generated from ScoutHealth must be treated as confidential.

Users must only download, export or print information where it is required for an approved Scouts Victoria purpose, such as:

- activity, camp or event planning.
- first aid preparation.
- emergency response.
- offline access where internet access may be limited.
- governance, audit, risk or compliance review.
- approved administrative purposes.

Users who download, export or print ScoutHealth information must:

- store the information securely.
- keep it out of public view.
- only share it with others on a strictly need to know basis
- avoid saving it to personal devices unless necessary and secure.
- not upload it to unauthorised platforms or generative AI tools.
- not send it through unsecured channels.
- delete or securely destroy it when no longer required.
- report any loss, unauthorised access or accidental disclosure immediately.

Printed health records used during activities, camps or events must be kept secure but accessible to authorised Leaders, first aid officers or designated safety personnel when required for health, safety or emergency response.

Storage and Security

Scouts Victoria must take reasonable steps to protect ScoutHealth information from misuse, interference, loss, unauthorised access, modification or disclosure.

ScoutHealth will be managed using appropriate technical and organisational security controls.

Users with access to the ScoutHealth system must not:

- share login details.
- use another person's account.
- attempt to bypass access controls.
- access records without authority.
- copy information into unauthorised systems.
- store exported information insecurely.
- leave printed records unsecured.
- disclose information to unauthorised people.

Data Quality, Review and Correction

Members and Parent are responsible for ensuring information entered into ScoutHealth is accurate, complete and current, and for keeping it up to date. ScoutHealth may include review dates, prompts or alerts to help identify information that may need updating. How individuals may access and seek correction of personal information held by Scouts Victoria is set out in the Scouts Victoria Privacy Policy 2026.

Disclosure of Information

Scouts Victoria does not intend to disclose information collected through ScoutHealth to third parties except as permitted under the Scouts Victoria Privacy Policy 2026. The circumstances in which information may be disclosed and the limits on any disclosure are set out in that Policy.

Overseas Disclosure and Data Residency

Information collected through ScoutHealth must not be intentionally transmitted or disclosed outside Australia except as permitted under the Scouts Victoria Privacy Policy 2026 and applicable privacy laws.

ScoutHealth must not be configured to intentionally transmit ScoutHealth data outside Australia for marketing, analytics, generative artificial intelligence, testing, development or

support purposes unless this has been assessed and approved through the appropriate privacy, legal and security review process.

Retention and Disposal

ScoutHealth records must be retained for as long as required to meet operational, legal, child safety, health, insurance and governance obligations.

Records must not be deleted, destroyed or permanently de-identified if they may be required for:

- an active or potential complaint.
- an incident or injury matter.
- a child safety concern.
- an insurance claim.
- legal proceedings.
- an investigation.
- an audit or governance review.
- a regulatory request.
- a data breach assessment.

The detailed retention schedule for ScoutHealth records, as approved by Scouts Victoria, is set out below.

The following minimum retention periods apply to ScoutHealth records:

Record type	Examples	Minimum Retention
Youth Member health records	Medical details, allergies, dietary needs, medication information, action plans	Until the member turns 25 or 7 years after last participation, whichever is longer
Adult Member health records	Medical declarations, emergency medical details, relevant activity health information	7 years after last participation
Incident and injury-related health records	Accident reports, emergency response records, first aid-related records linked to Health information	indefinitely
Child safety-related records	Disclosures, welfare concerns, reports or related records	indefinitely

Record type	Examples	Minimum Retention
Access and audit logs	Access logs, update logs, export logs, administrative activity	Until the member turns 25 or 7 years after last participation, whichever is longer.

As soon as practicable after the end of the minimum retention period, records must be securely deleted or destroyed in accordance with approved Scouts Victoria procedures, unless they are required to be retained for any of the purposes specified above

Disposal of ScoutHealth records must be authorised, controlled and documented. Records must not be destroyed informally or by individual users outside approved processes. For information on disposal of Sensitive documents please contact privacyofficer@scoutsvictoria.com.au

Data Breaches and Security Incidents

Any actual or suspected unauthorised access, disclosure, loss, misuse, interference, modification or compromise of ScoutHealth information must be reported immediately to the Privacy Officer or nominated Scouts Victoria contact.

Examples include:

- accessing a member's health record without authority.
- sending a report, PDF or export to the wrong person.
- losing printed health records.
- losing a device containing exported ScoutHealth information.
- suspected account compromise.
- unauthorised downloads, exports or screenshots.
- accidental disclosure of medical, allergy, disability or support information.
- unauthorised access by a former member, Leader, employee, volunteer, contractor, Parent.
- system vulnerability or security weakness that may expose ScoutHealth information.

Data breaches must be managed in accordance with Scouts Victoria's Data Breach Response Plan and applicable legal obligations.

Complaints and Enquiries

Privacy concerns, access requests, correction requests and complaints about ScoutHealth information should be directed to:

Privacy Officer
Scouts Victoria
Email: privacy.officer@scoutsvictoria.com.au
Mail: 152 Forster Road, Mt Waverley, 3149

If a person is not satisfied with Scouts Victoria's response, they may escalate the matter to:

- Office of the Australian Information Commissioner; or
- Health Complaints Commissioner, in relation to health information.

Roles and Responsibilities

Branch Executive Committee
Responsible for:

- approving this Policy.
- overseeing privacy, data governance and risk.
- ensuring appropriate governance, resources and controls are in place.
- monitoring significant risks, incidents and compliance issues.

Executive Manager / Privacy Officer
Responsible for:

- privacy guidance and oversight.
- managing privacy enquiries and complaints.
- coordinating data breach assessment and response.
- advising on access and correction requests.
- supporting privacy training and awareness.

ScoutHealth System Owner
Responsible for:

- operational governance of ScoutHealth.
- ensuring the system supports approved data management, privacy, access, retention and reporting requirements.
- coordinating privacy, security and child safety requirements with relevant teams.
- ensuring system changes consider privacy, security and child safety impacts.
- maintaining alignment between ScoutHealth, Collection Notice, Privacy Policy and approved procedures.

System Administrators
Responsible for:

- managing user access in accordance with approved processes.

- applying access changes when roles or membership status change.
- maintaining system configuration and security settings.
- supporting audit, reporting and incident response.
- using administrative access only for approved purposes.

Leaders, volunteers and employees
Responsible for:

- only accessing information required for their role.
- keeping information confidential.
- handling reports, PDFs, exports and printed records securely.
- using information only for approved Scouts Victoria purposes.
- reporting suspected breaches, incorrect access or security concerns immediately.
- following this Policy and related procedures.

Members and Parent
Responsible for:

- providing accurate and current information.
- reviewing and updating information when circumstances change.
- ensuring they have authority to provide information on behalf of a Youth Member.
- notifying Scouts Victoria where information is incorrect, incomplete or outdated.
- keeping their own account credentials secure.

Training and Awareness
Users who access ScoutHealth information should receive appropriate guidance on:

- privacy and confidentiality.
- appropriate access and use.
- handling health and sensitive information.
- secure use of reports, PDFs, exports and printed records.
- child safety and wellbeing obligations.
- data breach and incident reporting.
- account security.
- when information may and may not be disclosed.

Training and awareness may be delivered through induction, Leader guidance, system prompts, user guides, administrator procedures, refresher communications or formal training.

Monitoring and Compliance
Scouts Victoria may monitor access, updates, exports and administrative activity within ScoutHealth to support:

- system security.
- privacy compliance.
- child safety.
- investigation of suspected misuse.
- audit and governance.
- data quality and operational improvement.

Suspected misuse of ScoutHealth information may result in access removal, investigation, disciplinary action, membership action, reporting to relevant authorities or other action as appropriate.

Policy Review

This Policy will be reviewed:

- every two years.
- when there are material changes to ScoutHealth.
- when the Privacy Policy or Collection Notice is materially updated.
- following a significant privacy, security, health, safety or child safety incident.
- following relevant legislative, regulatory or operational changes.

Approval

POLICY OWNER: Brach Executive Committee
DATE APPROVED: June 16, 2026
REVIEW DATE: May 2028