

DIGITAL SYSTEM DESIGN PRINCIPLES

1. Digital safety by design and by default

We are committed to creating and maintaining safe, inclusive, and respectful digital environments for all young people involved in our organisation. We commit to digital safety by design and by default - meaning that child safety, wellbeing, and privacy are embedded into the planning, selection, use, and review of all digital systems, platforms, and practices from the outset, not added later. All end-users can use online services safely and children's best interests are a primary consideration in the design and operation of services likely to be used by children.

2. Buy before build; configure before customise and measurable outcomes

We prefer proven, upgradeable products. Use configuration and standard plugins first; avoid custom code unless it's genuinely strategic and sustainably funded. This reduces cost and upgrade risk while speeding delivery. Technology solutions must have measurable outcomes as part of the approval process (e.g., reduced cost, increased utilisation of digital platforms, compliance, etc).

3. Integration by design (API-first)

We select platforms with open, well-documented Application Protocol Interfaces (APIs) and event hooks. Use standard connectors before bespoke integration. Data should flow automatically between modules (membership, consent, events/contingents and finance) - no double entry.

4. Single source of truth & data quality

We define canonical records (people, roles, units, consents, events) with clear owners and lifecycle. We seek to "capture data once, reuse data everywhere". A time-boxed 60-day data cleanse is a pre-condition to any migration to Scouts Australia systems / applications.

5. Identity, access & privacy (secure by design and by default)

Our technology solutions require Single Sign On (SSO), least-privilege, Multi-Factor Authentication (MFA) for all roles, encryption in transit/at rest, audit logging, and rapid leaver de-provisioning. Youth identity data has real-world value — we protect it by design and by default, not as an afterthought to support safer, trusted Scouting.

6. Lowest sensible point of approval

We design workflows so decisions happen where the work is done: Units and event lead where appropriate, with clear guardrails. Fewer handoffs, fewer forms, less waiting.

7. Usability & accessibility first

Mobile-first, clear language, predictable steps, and good defaults. If a weekly hall night or camp signup is hard to do on a phone, we redesign it. The technology must be user friendly for our youth members and volunteers who have varying digital skills. It must integrate with existing systems and workflows. We green-light initiatives that show measurable member-experience gain (time saved, faster consent, better retention) and alignment to program outcomes. Systems must enable delivery of the Scouts Australia Member Experience Principles.

DIGITAL SYSTEM DESIGN PRINCIPLES

8. Reliability, sustainable and maintainable

Target >99.9% availability for core member/consent/event functions, auto-scaling for peaks (e.g., contingents), tested backups, and documented disaster recovery. Technology solutions must be able to be realistically supported and maintained in the long term. Vendor support, documentation and training must be readily available. There must be a clear plan / process for updates, backups and disaster recovery.

9. Risk and Compliance

Scouts Australia technology solutions must be regulatory compliant (including the Privacy Act 1988 (Cth) and any state-based regulations). Potential risks must be identified (cybersecurity, privacy, data protection and reputational).

10. Scalability & fair cost-to-serve (value for money)

We favour per-member economics that scale in large branches and don't penalise smaller ones. Use national volume and Not-for-Profits (NFP) arrangements to lower unit prices and keep costs predictable.

11. Change made easy

Every change ships with "what's changing/why/how", short training, and simple help paths. Pilot, measure, iterate and learn from mistakes. There MUST be a change management plan and a communications plan.