

SAINTS CATHOLIC COLLEGE

PRIVACY POLICY



Owner	CEO – Head of College
Status / approval	25 th September 2026
Review	January 2029 or following material legal, technological or operational change

1. PURPOSE AND APPLICATION

Saints Catholic College (SCC) protects the privacy and dignity of residents, applicants, families, employees, volunteers, contractors, visitors, alumni and others whose personal information it handles. This Policy governs collection, use, disclosure, security, retention, access, correction, complaints and data breaches. It applies to all workers and authorised users.

SCC operates within the Catholic Diocese of Townsville. This Policy is read with RCTC-P04_24 Privacy Policy, applicable privacy law and the 13 Australian Privacy Principles (APPs), to the extent applicable to SCC and the Roman Catholic Trust Corporation for the Diocese of Townsville (RCTC). Applicable law and binding Diocesan requirements prevail where requirements differ. This Policy is available free of charge on request and through SCC's published channels; reasonable requests for an accessible format will be considered.

2. ACCOUNTABILITY

- CEO – Head of College: accountable for privacy governance, serious incidents, exceptions, external notifications and required Diocesan reporting.
- Business Manager (Privacy Coordinator): manages privacy notices, information inventory, access controls, requests for access/correction, service-provider checks, breach records and coordination with the CEO.
- Department managers: restrict collection and access to business need, oversee relevant records and suppliers and promptly report suspected breaches.
- All workers and authorised users: protect information, verify recipients, use approved systems and immediately report loss, mistaken disclosure or suspicious access.

3. COLLECTION, ANONYMITY AND UNSOLICITED INFORMATION

SCC may collect identity and contact details; accommodation, guarantor and emergency-contact information; financial, study and residency records; recruitment, employment and training records; contractor induction and credentials (including PassTab and relevant Blue Card status); CCTV, access and incident records; and website or communication preferences. Where necessary and lawful, SCC may handle sensitive health, disability, religious, safeguarding or disciplinary information.

Collection must be lawful, fair and reasonably necessary for accommodation, pastoral care, safety, safeguarding, employment, contractor management, financial administration, events, communications or governance. Sensitive information generally requires consent unless a lawful exception applies. SCC collects directly from the individual where practicable and minimises the information collected.

Where lawful and practicable, individuals may deal with SCC anonymously or using a pseudonym, for example when making general enquiries. Identification may be required for accommodation contracts, payments, employment, safety or legal obligations. Unsolicited personal information must be assessed promptly: if SCC could not lawfully have collected it, SCC will destroy or de-identify it as soon as practicable where lawful and reasonable; otherwise it will be handled under this Policy.

4. COLLECTION NOTICES, USE AND DISCLOSURE

At or before collection, or as soon as practicable afterwards, SCC will take reasonable steps to explain the circumstances and purposes of collection, whether collection is required by law, consequences of non-provision, usual recipients, access and correction processes, complaint arrangements and how to obtain this Policy. SCC does not currently disclose personal information overseas. If information is obtained from another person, SCC will ordinarily notify the individual, subject to lawful exceptions.

SCC uses or discloses information for the collected purpose, a permitted related purpose, with consent or as required or authorised by law. Recipients may include the Diocese/RCTC, JCU where appropriate, advisers, insurers, payment and technology providers, emergency services and safeguarding or regulatory authorities. Significant or sensitive disclosures must be limited to what is needed and appropriately recorded. SCC does not sell personal information.

Marketing and alumni communications must meet applicable consent and direct-marketing rules, identify SCC and offer a clear, accessible opt-out; requests to stop marketing will be acted on within a reasonable period. Public photographs, video and resident stories require appropriate permission under the Media and Communications Policy, with safeguarding taking priority.

5. SECURITY, SERVICE PROVIDERS AND CROSS-BORDER SAFEGUARDS

- Use role-based access, strong authentication, approved devices and secure storage and transfer; restrict sensitive health, safeguarding, complaints, employee and financial records. Do not use personal accounts or unapproved applications for SCC records.
- Assess provider privacy and security arrangements, contractual controls and access before sharing information. Managers audit PassTab contractors monthly and resolve missing inductions or credentials before relevant onsite work.
- SCC does not currently disclose personal information to overseas recipients or use overseas data-handling arrangements. Any proposed overseas disclosure or overseas service-provider arrangement must be assessed and approved before implementation, including applicable APP 8 safeguards. SCC will update this Policy and relevant collection notices before any such arrangements commence, where required.
- Government-related identifiers (including Medicare and other government identifiers) must not be adopted as SCC identifiers or used/disclosed except where permitted by law. Tax file numbers are handled under their specific legal rules.

6. ACCURACY, RETENTION AND DISPOSAL

Managers take reasonable steps to keep information accurate, current and complete, and relevant when used or disclosed. SCC retains records only as required for their purpose and applicable statutory, employment, contractual, safeguarding and Diocesan obligations. The Business Manager maintains the retention schedule. When no longer required and lawful to dispose of, records are securely destroyed or irreversibly de-identified, including provider-held copies where practicable.

7. ACCESS AND CORRECTION

Individuals may request access to or correction of their personal information through the Business Manager using SCC's published contact details. SCC will verify identity, acknowledge and respond within a reasonable period, explain any lawful refusal or redaction in writing where required, and advise any lawful retrieval or copying fee in advance; no fee applies to making an access request. Where correction is disputed, SCC will record the request and, where appropriate, attach a statement of disagreement. On request, SCC will take reasonable steps to notify previous recipients of corrected information where required and practicable. Diocesan-held information will be coordinated with the Diocesan Office.

8. PRIVACY COMPLAINTS

Privacy concerns may be raised verbally or in writing with the Business Manager or CEO. The CEO is responsible for the SCC Complaints Register and will ensure privacy complaints are recorded and handled under the Complaints Management Policy, including acknowledgement, assessment, investigation, outcome, corrective action and escalation. Complaints involving the Business Manager go to the CEO; complaints involving the CEO follow the applicable Diocesan pathway. SCC will advise available external complaint avenues where applicable and refer APP or Diocesan-held-information concerns to the Diocesan Office as appropriate.

9. DATA BREACHES AND INCIDENTS

Suspected loss, unauthorised access, mistaken disclosure, cyber compromise or misuse must be reported immediately to the Business Manager and CEO. SCC will contain the incident, protect affected people, preserve

evidence, assess the impact, record decisions and remedy control failures. Where the Notifiable Data Breaches scheme applies, SCC will assess suspected eligible breaches within the statutory period and notify the OAIC and affected individuals as required. Other safeguarding, police, contractual and Diocesan reporting duties are assessed separately; urgent safety action must not be delayed. The CEO will promptly inform the Diocesan Governance Coordinator of non-compliance and escalate serious matters under RCTC-P04_24.

10. WEBSITE, CCTV AND SPECIAL HANDLING

Website administration access is restricted to the CEO and authorised third-party website managers, with appropriate security controls. CCTV and access records are used for legitimate safety, security and investigation purposes with signage, restricted access and defined retention. Children's, safeguarding, reportable conduct, health and pastoral-care information receives enhanced protection.

SCC does not currently use automated decision-making systems. Before introducing any system that uses personal information to make, or substantially assist with, decisions significantly affecting individuals, SCC will assess its privacy obligations and update this Policy where required, including applicable APP 1 transparency requirements.

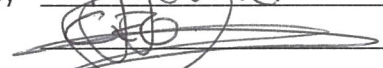
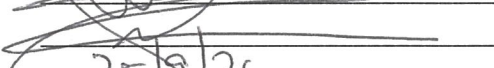
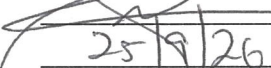
11. MONITORING, TRAINING AND REVIEW

Privacy training forms part of staff induction and is recorded in HR files. The Business Manager maintains evidence of access reviews, requests, provider checks, incidents and corrective actions. Department managers confirm staff awareness. The CEO reviews material incidents and systemic weaknesses and reports through the applicable governance pathway. Review occurs at least every three years or earlier following significant legal, technological or operational change.

12. RELATED DOCUMENTS

RCTC-P04_24 Privacy Policy; SCC Governance Framework; Complaints Management Policy; Media and Communications Policy; Reportable Conduct Scheme Procedure; contractor induction arrangements (PassTab); records-retention schedule; applicable Code of Conduct and Diocesan safeguarding, information-security and recordkeeping requirements; Privacy Act 1988 (Cth), APPs and Notifiable Data Breaches scheme where applicable.

13. POLICY ADMINISTRATION

Policy Owner CEO – Head of College
 Policy Consultation Business Manager / Key Stakeholders
 Policy Validation CEO – Head of College
 Authorised By 
 Position 
 Signature 
 Date 
 Effective Date 25th September 2026
 Next Scheduled Review January 2029 or earlier if required
 Version 2.2 – Draft for approval

VERSION HISTORY

Version	Date	Enacted Date	Comments
2.0	August 2026	Amended	Privacy Policy draft
2.1	September 2026	Approved	Expanded APP coverage and clarifications
2.2	September 2026	Approved	Confirmed no overseas data handling or automated decision-making; retained controls for future changes