SCAC	Document Control
Document title	CRCA Internet Usage Policy
Document identifier	SCAC-Pol-13-IUP
Document owner	Safe Church Advisory Committee
Approved by	SCAC & Synodical Interim Committee (Interim approval)
Version	1.0
Date approved by SCAC	16 September 2026
Next review date	15 September 2028
Authoritative location	www.safechurch.crca.org.au/documents
Document status	Controlled

Contents

1. PURPOSE 2
2. BIBLICAL AND THEOLOGICAL BASIS 2
3. SCOPE 2
4. VALUES 2
5. DEFINITIONS 2
6. POLICY 3
7. PROCEDURES 3
8. ROLES AND RESPONSIBILITIES 4
9. BREACHES 4
10. RELATED POLICIES 4
11. MONITORING AND REVIEW 5

1. PURPOSE

1.1. To ensure that internet usage within the CRCA upholds safety, respect and Christian values, and protects all people, especially children and adults at risk, when using digital environments connected with CRCA activities.

2. BIBLICAL AND THEOLOGICAL BASIS

2.1. James 3:13 calls wisdom to be shown through good conduct and humility. Internet use connected with CRCA activities is part of Christian witness and should reflect wisdom, restraint and care.

2.2. Colossians 3:17 reminds the church that words and actions are to be done in the name of the Lord Jesus. Online communication is therefore to honour Christ and protect the dignity and safety of others.

3. SCOPE

3.1. This policy applies to all members, pastors, elders, staff, volunteers, contractors and affiliates of the CRCA when using CRCA networks, devices, official accounts, online systems or any internet activity connected with their association with the CRCA. It does not restrict ordinary public access to CRCA websites; it governs use, administration, publication and conduct connected with CRCA roles, activities, networks, systems or official channels.

3.2. This policy also applies to the digital handling of safeguarding incidents, reports, complaints, records and related information.

4. VALUES

4.1. The CRCA is committed to the following values so that the safety and well-being of all people remain at the forefront of decisions and actions.

4.1.1. **Scriptural teachings - upholding safety and dignity:** central to the Church's teaching is the call to embody love, mercy and justice. Colossians 3:17 calls all things to be done in the name of the Lord Jesus, and Luke 18:16 shows Jesus welcoming children and affirming their place in the kingdom. The responsibilities in this policy are therefore carried out in a way that honours the dignity, voice and safety of each person.

4.1.2. **Zero tolerance:** the CRCA has a zero-tolerance approach to abuse and harmful behaviour. The responsibilities in this policy must never be used to suppress, minimise or ignore concerns about safety, harm or abuse.

4.1.3. **Transparency and accountability:** the CRCA fosters a culture of openness, appropriate information sharing, feedback and accountable action.

4.1.4. **Shared responsibility:** safeguarding is everybody's responsibility and requires the participation of local churches, personnel, members and denominational safeguarding structures.

4.1.5. **Empowerment:** the CRCA supports people to understand their rights, speak up, raise concerns and contribute to the development of safer church environments.

4.1.6. **Integrity:** the CRCA fosters honest, ethical and respectful engagement at all levels of church life.

5. DEFINITIONS

5.1. Terms defined in the National Safeguarding Policy apply to this policy unless this section gives a more specific operational meaning.

5.2. **CRCA system** means an internet, email, website, platform, account, device, data-storage location or digital service used for CRCA ministry, governance, communication, administration or safeguarding purposes.

5.3. **Internet use** means access to or use of websites, online services, email, messaging, applications, cloud storage, digital platforms or other internet-enabled resources in a CRCA context.

5.4. **Online communication** means communication through email, messaging, websites, online services, applications, forums, video calls or other digital channels.

5.5. **Device** means a computer, tablet, phone, storage device or other equipment used to access a CRCA system or online service.

5.6. **Unsuitable content** means content that is abusive, exploitative, sexualised, violent, discriminatory, harassing, unsafe, unlawful, contrary to this policy, or inconsistent with a safe CRCA environment.

5.7. **Digital safeguarding risk** means a safeguarding risk arising from online access, online communication, digital content, device use, data management, visibility, supervision, privacy, or contact with children or adults at risk online.

5.8. **Public online service** means a website, platform or online service that is available to members of the public and may be accessed without becoming a CRCA-controlled system user.

5.9. **Monitoring** means authorised checking, logging, review or investigation of CRCA system use for safeguarding, security, policy, legal or operational purposes.

6. POLICY

6.1. **Ethical online conduct:** all internet use connected with CRCA activities must reflect Christian faith, integrity, respect and the safeguarding commitments of the CRCA.

6.2. Statutory framework for online safety: the CRCA's online and digital practices are conducted consistently with the Online Safety Act 2021 (Cth), the eSafety Commissioner's guidance for organisations and other applicable online safety requirements.

6.3. **Safe data management:** personal, sensitive and church-related information must be protected from unauthorised access, misuse, loss, disclosure and other digital risks. Personnel must not enter personal or sensitive information into public or other online services where confidentiality, retention or onward use cannot be controlled.

6.4. Respectful communication: all online communication connected with CRCA activities must be civil, constructive and free from bullying, harassment, intimidation, image-based abuse or other harmful conduct.

6.5. **Content restrictions:** personnel and members must not use CRCA networks, systems or official channels to access, create, distribute or promote content, including digitally created or altered content, that is unlawful, abusive, sexually explicit, exploitative, discriminatory, unsafe or contrary to CRCA safeguarding commitments.

6.6. Image-based abuse: non-consensual sharing or threatened sharing of intimate images is contrary to this policy and the Code of Conduct. Where such conduct is alleged, the matter is responded to under the Complaints Handling Policy and the Disciplinary and Breach Response Policy, and is reported to the eSafety Commissioner and Police as required by the circumstances.

7. PROCEDURES

7.1. **Account management:** official CRCA accounts are clearly distinguished from personal accounts. Account profiles and privacy settings must not disclose personal, sensitive or private information unnecessarily.

7.2. **Data security:** CRCA internet use is supported by appropriate password protocols, multi-factor authentication where available, password management, software updates and device security standards.

7.3. **Use of CRCA systems:** people using CRCA networks, devices or official accounts must do so only for appropriate ministry, church, employment, volunteer or approved activity purposes, and must not intentionally compromise security or confidentiality.

7.4. **Adult-to-child digital communication:** adult-to-child direct messaging and other one-to-one digital communication are governed by the Social Media Policy and the Code of Conduct. Personnel do not use personal accounts for one-to-one communication with children in connection with CRCA activities.

7.5. **Image publication consent:** consent to take an image and consent to publish it are treated as separate permissions. Image publication consent is governed by the Social Media Policy, the Code of Conduct and the Privacy Policy.

7.6. **Reporting concerns:** concerns about internet use may be raised with local church leadership, the Safe Church Representative, or the Safe Church Unit where safeguarding response support, triage assistance or escalation is required. Serious, sensitive or misconduct-related concerns may also be raised under the Whistleblower Policy, Complaints Handling Policy or Disciplinary and Breach Response Policy, as appropriate.

7.7. **Training and awareness:** internet safety, online conduct, privacy and digital safeguarding are included in relevant safeguarding training under the Learning and Development Policy. Additional guidance may be provided through newsletters, local church communication or CRCA resources.

8. ROLES AND RESPONSIBILITIES

8.1. Role definitions used in this policy are consistent across the CRCA policy suite.

8.2. **Session / Church Council:** supports safe local internet practice; authorises official local-church digital channels; ensures local leaders and account administrators understand this policy; manages local account-access arrangements; and responds to local internet-use concerns through the appropriate safeguarding, complaints or governance pathways.

8.3. **Safe Church Representative:** assists local people to understand how internet-related safeguarding concerns can be raised and referred through the CRCA safeguarding pathways. The Safe Church Representative may support local follow-up where authorised by the Session / Church Council.

8.4. **Safe Church Administrator:** supports administrative, training-record, resource and document-control functions relevant to internet safety, including approved templates, guidance material, training resources, accessible resources and central records where required by the CRCA safeguarding framework.

8.5. **Safe Church Unit:** provides safeguarding response advice, triage assistance and escalation support where internet-related concerns involve harm, risk, complaints, disclosures, statutory reporting, Police matters, privacy / information-sharing matters or other safeguarding pathways. The Safe Church Unit supports, but does not replace, local church governance responsibility for local internet use or account administration.

8.6. **Safe Church Advisory Committee:** provides oversight, policy direction and quality-improvement review for internet-safety matters through the Continuous Quality Improvement Policy.

8.7. **Personnel, members and authorised account administrators:** use internet systems safely, maintain appropriate account security, uphold this policy, and report concerns or breaches.

9. BREACHES

9.1. Breaches of this policy are dealt with under the Disciplinary and Breach Response Policy. Serious breaches may also involve complaints handling, whistleblower protections, Police reporting, eSafety reporting, privacy / information-sharing obligations or legal action as required by the circumstances and the CRCA Church Order.

10. RELATED POLICIES

10.1. National Safeguarding Policy. Code of Conduct. Social Media Policy. Privacy Policy. Information Sharing and Record Keeping Policy. Complaints Handling Policy. Whistleblower Policy. Disciplinary and Breach Response Policy. Learning and Development Policy. Engagement Policy.

11. MONITORING AND REVIEW

11.1. This policy is reviewed every three years, or earlier where required by legislative change, regulator guidance, audit findings, serious incidents, a substantiated complaint, material safeguarding risk, or a decision of the Safe Church Advisory Committee. Feedback on this policy may be sent to the Safe Church Unit at scu@crca.org.au at any time.

Document	Control	History			
Version	Approval date	Effective date	Approved by	Author or review lead	Summary of changes
0.1	16/09/2025	16/09/2025	Not approved	Align Safeguarding	Initial consultation draft.
0.2	09/07/2026	09/07/2026	SCAC	Align Safeguarding	Statuary updates
0.3	28/07/2026	28/07/2026	SCAC (SIC)	Align Safeguarding	SCAC feedback
1.0	16/09/2026	16/09/2026	SCAC (SIC)	Align Safeguarding	First approved issue.