SCBC ICT Acceptable Use Policy

SOUTH COAST
BAPTIST COLLEGE

This policy outlines how South Coast Baptist College (SCBC) expects its community members to behave with technology. The purpose of this policy is protecting our community, providing an effective learning environment, and maintaining a secure and reliable network. Information and Communication Technology (ICT) refers to all computer hardware, software, systems, networks, and telecommunication devices or services used or accessed within the College campus or connected to the College in any way.

This policy applies in conjunction with the Privacy Act 1988 (Cth), Cybercrime Act 2001 (Cth), Criminal Code (WA), Censorship Act 1996 (WA), Equal Opportunity Act 1984 (WA), Freedom of Information Act 2010 (Cth), and the Copyright Act 1968 (Cth).

- All ICT relating to SCBC is for educational purposes only, they are not to be used for conducting private matters or for entertainment purposes.
- Use of student home drives, student emails or any other method of storage or communication provided by the college is as educational material only.
- The College retains the right to install management software, applications, packages, and updates to any device on the College network.
- All ICT equipment should be treated with care, and any damage promptly reported to a teacher.
- Specific personal ICT devices are only allowed to access the College network when explicitly authorised by the College. This rule relates to specific year groups and very specific circumstances. Any devices not authorised for use on the College network are liable to be confiscated.
- The College retains the right to check all written, graphic, audio, and other materials created, produced, communicated, stored, or accessed within the College community. This includes materials on College ICT equipment, any personal devices used on the College campus, and external online services provided by the College. This can occur with no prior warning, at any time.
- Community members should make no attempt to remove, bypass, or circumvent any security, filtering or monitoring put in place by the College.
- Any community member's actions that degrade the network performance in any way may have their ICT access restricted or removed.
- Various data logs are retained for over 12 months and can be reviewed for rule breaches, with the possibility of retrospective disciplinary action.
- Community members shall take personal responsibility when using the College's ICT infrastructure. They must protect their personal information and data, maintaining a high level of security to avoid compromising their own safety and the safety of other members of the community.
- Community members must take reasonable measure to ensure they do not bring any software on to the College network that could create a security risk to the community.
- Community members should be respectful of others online privacy at all times, both on and off College campus.
- Transmitting or deliberately accessing inappropriate material is not tolerated. This includes (but is not limited to) threatening, sexually explicit, harassing, offensive or discriminatory materials.
- Bullying or harassment of any community members and anyone external to the College is not tolerated.
- If a community member is issued login details they are to retain and not disclose those details to anyone else. Members attempting to use other members login details will face disciplinary measures.
- College owned ICT equipment is not to be removed from the campus, except with explicit permission.
- The College will not be responsible for the loss, misuse or damage of any personal ICT devices.

Any breaches of the acceptable use policy can result in disciplinary action and/or restriction from the College ICT infrastructure. Severe breaches (as decided by the Assistant Principal) can result in immediate expulsion and a report made to appropriate State authorities.