

QCBC Information Technology Policy

Aim: To protect the integrity of the IT systems at QCBC so that they are always fully functioning.

The Board limits the use of the club's IT equipment to authorised people. The IT sub-committee of the QCBC board maintains a list of those authorised users. The Board limits a person's access to specific pieces of equipment.

Table 1 Authorised Usage of Specific Equipment	
Specific Equipment	Authorised Users
Dealing PC	Dealers and Teachers
Dealing Boards	Dealers and Teachers (formal permission is required to remove the boards and/or cards from QCBC premises)
Bridgemate PC	Directors and Compscore3 Application Users
Clock PC	Directors and Compscore3 Application Users
Chromecast	External users such as Congress Directors, Teachers and Meeting Organisers may use the Chromecast facilities.
Printers	External users such as Congress Directors, Teachers and Meeting Organisers may use the QCBC printers.
South TV	Mainly used by Directors but may be used by visiting external organisations subject to specific approval. The visitor may move the TV but must return it to its original place in its original condition. This includes returning the power cord, extension cords, power boards, remote control and Chromecast.

Acceptable Use of IT Equipment

Users must:

- Use IT equipment for QCBC business purposes only.
- Keep equipment in good condition and report any damage, loss, or theft immediately.
- Follow all licensing agreements and copyright laws.
- Log off or lock devices when unattended.

Users must not:

- Install unauthorized applications.
- Connect any devices, including flash drives, to QCBC computers.

IT Security Requirements

All users must:

- Keep login credentials confidential.
- Log out of critical and sensitive applications (e.g. MyABF) once activities are completed.
- Comply with QCBC's Authentication procedures.
- Report any security incidents/suspicious behaviour to a member of the IT committee or the Office Manager.

Prohibited security behaviours

- Bypassing security controls or modifying system configurations without approval.
- Storing sensitive QCBC data on personal devices or unapproved cloud services.

Remote Work and Mobile Device Usage

- Access to QCBC systems from remote locations must occur through secure, approved channels (e.g. Splashtop Business).
- Mobile devices must be protected with a passcode and encryption.
- Lost or stolen devices must be reported immediately.

Monitoring and Privacy

- QCBC reserves the right to monitor all IT systems and data to ensure compliance.
- Users should have no expectation of privacy when using company-owned equipment or networks.

External Users

External users are governed by this policy. Any external user that creates IT work for QCBC may have to pay for that work by having an amount deducted from their fee.

Enforcement

Violations of this policy may result in disciplinary action at the discretion of The Board.

IT Committee

5 August 2025