Darling Downs Potters' Club Ltd

IT Security and Acceptable Use Policy

1. Purpose

The purpose of this policy is to ensure the secure, responsible, and appropriate use of the Darling Downs Potters' Club's IT systems, accounts, and data.

This policy aims to:

- Protect Club systems and information from unauthorised access
- Promote good password hygiene and account security
- Ensure accountability through individual user access
- Reduce risks associated with shared accounts and poor security practices

2. Scope

This policy applies to all individuals who are granted access to Club IT systems, including:

- Board members
- Members and Volunteers with authorised system access (e.g. POS systems, email, Social media and cloud services)

3. Policy Statement

All users must access Club systems securely and responsibly.

Shared accounts are to be avoided wherever possible. Individual accountability and basic security practices are required at all times.

4. User Accounts

4.1 Individual Accounts

- Each user must be provided with their own unique account where the system supports it.
- Shared accounts must not be used unless there is no technical alternative.

- User accounts must not be shared between individuals.

4.2 Access Control

- Where the system supports it, the principle of least privilege must be applied so users are granted only the minimum level of access required to perform their role.
- Access must be removed promptly when no longer required (e.g. volunteer leaves role).
- The Board will oversee and approve access to critical systems.

5. Password Requirements

All users must follow these password practices:

- Passwords must be **strong and unique**
- Passwords must not be reused across multiple systems / account
- Passwords must not be shared with other users
- Passwords must not be written down in visible or insecure locations

Recommended password standards:

- Minimum 12 characters
- Use a mix of words (passphrases are encouraged)
- Avoid easily guessed information (names, birthdays, etc.)

6. Password Management

- Where possible, users should use a reputable password manager to store passwords securely.
- The Club's administrator or shared critical accounts must be stored in a password manager controlled by the Board.
- Access to shared credentials (where unavoidable) must be limited and controlled by the Board.

7. Administrator Accounts

- Systems must have at least one administrator account controlled by the Board.

- Administrator credentials must:
    - Be stored securely in a password manager
    - Not be used for everyday activities
    - Only be accessed when required for administration tasks
- Where possible, separate standard user and admin accounts should be used.

8. Acceptable Use

Users must:

- Use Club systems only for legitimate Club purposes
- Log out of shared or public devices after use
- Take reasonable care when accessing systems on personal and shared devices
- Report any suspicious activity or potential security issues to the Board

9. Non-Compliance

Failure to comply with this policy may result in:

- Removal of system access
- Restrictions on volunteer duties
- Disciplinary action as determined by the Board

Serious breaches may result in further action where appropriate.

10. Review

This policy will be reviewed every two years or sooner if legislative or operational requirements change.