

BARCOO SHIRE COUNCIL POLICY ***INTERNET AND EMAIL USAGE***

| | |
|--|--|
| Policy Number: BSC-043 | Version: |
| Classification: Administrative | Section: Corporate Services - IT |
| Date Adopted by Council: 22 October 2019 | Resolution Number: 2019.10.019 |
| Responsible Officer: Chief Executive Officer | <p>Review: Note: This Policy is reviewed when any of the following occur:</p> <ol style="list-style-type: none"> 1. The related information is amended or replaced. 2. Other circumstances as determined from time to time by the Chief Executive Officer. <p>Notwithstanding the above, this Policy is to be reviewed at intervals of no more than two years.</p> |
| Legislation: | |

OBJECTIVE

The aim of this policy is to provide a framework for appropriate access to and use of the Barcoo Shire Council's (BSC) internet and email systems.

POLICY STATEMENT

The Internet and Email Usage Policy applies to the accessing of the internet and email systems by all employees in the performance of their work, specifically this includes:

- Internal and external email traffic;
- Internet access;
- Network access.

DEFINITIONS

Nil

POLICY

The BSC is committed to providing its staff with appropriate corporate applications and business tools, including access to internet and email systems, provided that employees use the internet responsibly and productively. Internet access is limited to job related activities only and personal use is limited to breaks such as morning/afternoon tea, lunches and after working hours with prior approval. Job related activities could include research and educational tasks that may be found via the internet that would help in an employee's role.

All internet data that is composed, transmitted and/or received by the BSC computer system is considered to belong to the BSC and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other third parties.

The equipment, services and technology used to access the Internet are the property of the BSC and BSC reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.

Emails sent via the emails system should not contain content that is deemed to be offensive. This

includes, though is not restricted to, the use of vulgar or harassing language or images.

Any downloads may be monitored and/or blocked by the BSC if they are deemed to be harmful and/or not productive to business.

The installation of any third party software is strictly prohibited without approval from the Director of Corporate Services (DCS).

Unacceptable use of the internet by employees includes, but is not limited to:

- Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material.
- Sending or posting discriminatory, harassing, or threatening messages or images on the internet or via the BSC email service.
- Using computers to perpetrate any form of fraud, and / or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorisation.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation.
- Sharing confidential material, trade secrets, or proprietary information outside of the organisation.
- Hacking into unauthorised websites.
- Sending or posting information that is defamatory to the BSC, its products/services, staff, communities, contractors and / or customers.
- Introducing malicious software onto the BSC's network and / or jeopardising the security of the BSC's electronics communication systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the BSC.
- Employees should only connect personal devices to the Barcoo Guest wifi.

If an employee is unsure about what constitutes acceptable internet usage, then they should ask their supervisor for further guidance and clarification.

Violations of this policy could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations in relation to their conduct. All employees are required to acknowledge receipt and confirm that they have understood and agreed to abide by this policy.

ASSOCIATED DOCUMENTS AND POLICIES

Social Media Policy