General Policy
Burke Shire Council
Computer and Telecommunication Resource Usage Policy

Document Details

Policy Reference Number:	ADM-POL-003
Version Number:	4
Next Scheduled Review Date:	31 March 2028
Status	Adopted
Category	General
Document ID number	94580

Approval

Council Resolution	Date	Reason / Comments
250324.17	24/03/2025	Revised Policy

Contents

Version History

Council Resolution	Date	Reason / Comments
10.120215	15/02/2012	New policy
15.150416	16/04/2015	Updated
190620.14	20/06/2019	Reviewed
220127.10	27/01/2022	Reviewed
230424.09	24/04/2023	Reviewed

1. Purpose

The purpose of this policy is to ensure that Burke Shire Council (Council) ICT and Telecommunication resources are used:

- Appropriately and efficiently;
- To assist Council to effectively deliver quality, value for money services;
- To not create or increase risk to Council, Council employees, Councillors, contractors and third parties;
- In accordance with other policies, legislation, standards, and business best practice; and
- Managed with sound consistent governance across Council.

2. Scope

This policy applies to all employees, councillors and contractors working for Council regardless of whether they are permanent, temporary, full time, part time or casual employees or volunteers. For the purposes of this policy, the term contractor includes on-hired temporary labour services (agency staff) and sub-contractors. This policy also applies to all people who use Council's Computer Network by any means (Users). The policy also applies to Users who contribute to external blogs and sites that identify themselves as with Council.

3. Date of Policy

This Policy applies from the date adopted by Council.

4. Definitions

Act	means the *Local Government Act 2009 (QLD)*.
Business Use	means council's corporate Internet, and email systems and associated services are established and maintained solely for Council related business purposes.
Call Diversion	means an automatic diversion of a call from the called extension to another number.
Call Pickup	means the ability to dial a number to pick up a call on another extension.
CEO	means Chief Executive Officer.
Chain Email	means an email directing recipients to send out multiple copies of it so its circulation increases exponentially. Such messages typically promise rewards for compliance, e.g. blessings, good luck, money or merchandise. Some types of chain letters - specifically, those asking people to send money to other participants - are illegal and not in accordance with Council policy.

Corporate Information	refers to all records and their associated contextual information that serves to completely depict all details of a particular business activity and its relationship to other business activities.
Corporate Memory	means a full and accurate record of all the business activities and transactions undertaken by Council in the exercise of its statutory, administrative or other public responsibilities or related purposes.
Council	shall mean the Mayor and Councillors of Burke Shire Council.
Councillor	shall mean a Councillor of a Burke Shire Council within the meaning of the *Local Government Act 2009*, includes the Mayor.
Electronic Correspondence	means any correspondence facilitated by ICT resources.
Electronic Storage Devices	means Personal Digital Assistants and handheld devices, USB Drive/Flash Keys, SD Cards, Portable hard drives/CD Burners, Zip Drives, Mobile Phones).
Email System	means a software application that provides services related to the transmission and receipt of electronic messages.
End-user Devices	are defined as Standard desktop computer, Standard notebook (portable) computer, various computer (PC) models, other mobile computing devices, printers, smart phones, Blackberrys, etc.
Employees	shall mean all persons employed at Burke Shire Council on a permanent, temporary, volunteer or casual basis and may include persons engaged under a contract of service.
ICT	means Information Communication Technology.
Malicious Software (Malware)	means that software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.
Peripheral Device	means a device that is optional in nature, and is attachable to an end-user device e.g. USB Drives, external hard drives, scanners and cameras.
Programmable Devices	means any device whose operation is controlled by a stored program that can be changed or replaced. Information may comprise automated software, data files and temporary work files. Such devices would include desktop computers, mobile communications devices, SCADA devices or even a modern refrigerator.
Regulation	means the *Local Government Regulation 2012 (Qld)*.

SPAM	means an unsolicited message that is sent indiscriminately to multiple mailing destinations.
Tethering/Tethered	means connecting a data-enabled mobile telephone or tablet device to a computer or other device via a cable or wireless connection for the purpose of connecting to the Internet via the phone/tablets' data connection.
User	means any authorised Council staff member, Councillor, contractor or third party.
Virus	means a software agent that uses any programmable device that is available to reproduce itself and spread itself to other programmable devices.
Voice Mail	means the ability to store a message for an extension that can be replayed at a later time.

5. Policy Provisions

Council ICT Resources are to be used in an ethical and efficient manner within a sound governance framework, thereby enabling Council's assets to be appropriately managed within acceptable risk tolerances. A key underpinning goal of this approach is to ensure users of ICT resources behave in ways that support the business activities of Council.

This policy aligns with Queensland Governments Information Standard - IS 38 – Use of ICT Facilities and Devices.

The provision of Council owned ICT resources including Internet, email facilities, telephony and devices are to be used for officially approved purposes. Limited personal use of ICT resources is available only in accordance with the uses outlined in this policy.

Council employees, consultants, contracted external service providers and Councillors are all required to use Council ICT resources in accordance with this policy and the applicable Code of Conduct.

All access to ICT resources is granted on the basis of business need and may be revoked at Managements discretion at any point in time.

5.1 Use of Internet, Email and Computers

(a) Where use is allowed, Users are entitled to use Council's Computer Network only for legitimate business purposes.

(b) Users are permitted to use Council's Computer Network for limited and reasonable personal use and only outside of normal hours of work. However any such personal use must not impact upon the User's work performance or Council resources or violate this policy or any other Council policy.

(c) A User must not use Council's Computer Network for personal use if that use interferes with the efficient business operations of Council or relates to a personal business of the User.

(d) Council gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any User in the course of using the Computer Network for the User's personal purposes.

(e) It is strongly recommended that users do not use Council's email system for personal or sensitive messages as all council emails constitute official public records unless containing private sensitive information in accordance with the Information Privacy Act.

(f) Council's electronic communications system must not be used to conduct private business, gamble or carry out excessive or regular research into non-work related topics.

5.2 Requirements for Use

Users must comply with the following rules when using Council's Computer Network:

(a) Users must use their own username/login code and/or password when accessing the Computer Network;

(b) Users in possession of Council electronic equipment must at all times handle the equipment in a responsible manner and ensure that the equipment is kept secure;

(c) Users must protect their username/login code and password information at all times and not divulge such information to any other persons. Where a person suspects that their password has been compromised it their responsibility to change it immediately;

(d) Users must not use another User's Computer Network facilities (including passwords and usernames/login codes) for any reason;

(e) Passwords must be changed whenever:

- The computer system automatically prompts the user to do so;
- In the absence of the user, an administrator has needed to use the users profile and has reset their passwords to do so;
- A user is requested to do so by the IT Support or Manager.

(f) Users should ensure that when not in use or unattended, the computer system is locked;

(g) A disclaimer is automatically included in all Council emails, and must not be removed;

(h) If a User receives an email which the User suspects contains a virus, the User should not open the email or attachment to the email and should immediately contact IT Support for assistance;

(i) If a User receives an email the content of which (including an image, text, materials or software) is in breach of this policy, the User should immediately report the matter to IT Support. The User must not forward the email to any other person;

(j) Users of the internet, telecommunications and email shall be accountable for the appropriate use of these technologies and must abide by the policies and principles outlined herein;

(k) New Users shall be provided with a user account when:

- The relevant manager has authorised access for the user; and
- The relevant manager has provided the required account information to build the new account profile; and

(l) All new users must read and acknowledge that they have read and understood Councils Computer and Telecommunication Resource Usage Policy.

5.3 Prohibited Conduct

Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on Council's Computer Network that:

(a) is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL). For example, material of a sexual nature, indecent or pornographic material;

(b) causes (or could cause) insult, offence, intimidation or humiliation;

(c) may be defamatory or could adversely impact the image or reputation of Council. A defamatory message or material is a message or material that is insulting or lowers the reputation of a Person or group of people;

(d) is illegal, unlawful or inappropriate;

(e) affects the performance of, or causes damage to Council's Computer System in any way; or

(f) gives the impression of or is representing, giving opinions or making statements on behalf of Council without the express authority of Council. Further, Users must not transmit or send Council's documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

Users must not use Council's Computer Network:

(a) to violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using Council's computing facilities, except as permitted by law or by contract with the owner of the copyright;

(b) to create any legal or contractual obligations on behalf of Council unless expressly authorised by Council;

(c) to disclose any Confidential Information of Council or any customer, client or supplier of Council's unless expressly authorised by Council;

(d) to install software or run unknown or unapproved programs on Council's Computer Network. Under no circumstances should Users modify the software or hardware environments on Council's Computer Network;

(e) to gain unauthorised access (hacking) into any other computer within Council or outside Council, or attempt to deprive other Users of access to or use of Council's Computer Network; or

(f) to send or cause to be sent chain or SPAM emails in any format.

Users must not use council mobile phones for the following prohibited activities:

(a) Viewing, creating, downloading, storing or distributing materials in the workplace which are inappropriate, indecent, obscene or sexually explicit, e.g., pornography;

(b) Taking inappropriate pictures with cameras or mobile phone cameras;

(c) Using Council phones to call private mobile phone numbers where it is not an emergency situation;

(d) Any use that incurs additional data charges to Council including but not limited to 'tethering' of non- Blackberry data devices and using Council-supplied mobile data as a replacement for a private Internet connection;

(e) Forwarding inappropriate jokes, image/sound/movie files, e.g., .WAV and .MPG files;

(f) Conducting private business enterprises for personal gain or profit;

(g) Downloading, storing or distributing material such as chain letters or information pertaining to pyramid schemes;

(h) Creating and/or maintaining personal websites;

(i) Knowingly downloading files from the Internet or storage media containing malicious code, viruses, Trojan horses, worms or Spyware that may cause harm to Council;

(j) Making telephone or mobile telephone calls to subscription numbers (e.g., 1900 numbers) or overseas/IDD numbers where specific exemption has not been authorised;

(k) Failing to keep Council passwords secure;

(l) Expressing a view to the media outside of an authorised delegation;

(m) Disrupting other ICT resources through such means as mass mailing, storage or transmission of large files or any other unnecessary activity that may place a burden on Council resources.

5.4 Security

(a) Users shall not disable, enable or interfere with software settings designed to improve security or protect the network from malicious attack.

(b) Users must not knowingly obtain unauthorised access to information (including passwords) and must not damage or delete, insert or alter information with malicious intent.

(c) Except where otherwise approved by the IT Support/Manager or the CEO, no user shall log on to the system for another person whether that person has a valid account or not.

(d) All users shall log off or “lock” their computer when they move away from their computer for an extended period.

(e) Users shall not install new applications or transfer any executable files to any Council computer without the approval of the IT Support/Manager.

5.5 Password Policy Requirements

(a) Password to all systems should be revised at minimal every 90 days and no greater than 180 days

(b) Passwords should be at least 12 characters long but 14 or more is better.

(c) Passwords should be a combination of uppercase letters, lowercase letters, numbers, and symbols.

(d) Passwords should be not a word that can be found in a dictionary or the name of a person, character, product, or organization.

(e) Passwords should be significantly different from your previous passwords.

(f) Easy for you to remember but difficult for others to guess. Consider using a memorable phrase like "6MonkeysRLooking^".

(g) Where possible, multifactor authenticators should be used to protect users from password breaches and to alert the user of any unauthorised access to systems.

5.6 Password Lock-out Thresholds

(a) Council will endeavour to implement 3 strike lockout threshold on all system where practicable.

(b) Where a user is locked out; Council will configure this to no longer than 15 minutes or by release of account lock by the network or system administrator .

5.7 Details on Blocking Email or Internet Access

Council reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a User, or access to an internet website by a User, if the content of the email or the internet website is considered:

(a) obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an e-mail message or in an attachment to a message, or through a link to an internet website (URL). For example, material of a sexual nature, indecent or pornographic material;

(b) causes or may cause insult, offence, intimidation or humiliation;

(c) defamatory or may incur liability or adversely impacts on the image or reputation of Council. A defamatory message or material is a message or material that is insulting or lowers the reputation of a Person or a group of people;

(d) illegal, unlawful or inappropriate;

(e) to have the potential to affect the performance of, or cause damage to or overload Council Computer Network, or internal or external communications in any way; or

(f) to give the impression of or is representing, giving opinions or making statements on behalf of Council without the express authority of Council.

In the case that an email is prevented from being delivered to or from a User, the User will receive a prevented delivery notice. The notice will inform the User that the delivery of the email has been prevented. The notice will not be given if delivery is prevented in the belief that:

(a) the email was considered to be SPAM, or contain potentially malicious software; or

(b) the content of the email (or any attachment) would or might have resulted in an unauthorised interference with, damage to or operation of any program run or data stored on any of Council's equipment; or

(c) the email (or any attachment) would be regarded by a reasonable Person as being, in all the circumstances, menacing, harassing or offensive.

Council is not required to give a prevented delivery notice for any email messages sent by a User if Council is not aware (and could not reasonably be expected to be aware) of the identity of the User who sent the e-mail or is not aware that the e-mail was sent by the User.

5.8 Computer Surveillance in Council's Workplace

On a continuous and ongoing basis during the period of this policy, Council will carry out Computer Surveillance of any User at such times of Council's choosing and without further notice to any User.

Computer Surveillance occurs in relation to:

(a) storage volumes;

(b) internet sites - every web site visited is recorded including the time of access, volume downloaded and the duration of access;

(c) download volumes;

(d) suspected malicious code or viruses;

(e) emails - the content of all emails received, sent and stored on the Computer Network. (This also includes emails deleted from the Inbox); and

(f) computer hard drives - Council may access any hard drive on the Computer Network.

Council retains logs, backups and archives of computing activities, which it may audit. Such records are the property of Council, are subject to State and Federal laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

Council may use and disclose the Computer Surveillance records where that use or disclosure is:

(a) for a purpose related to the employment of any employee or related to Council's business activities; or

(b) use or disclosure to a law enforcement agency in connection with an offence; or

(c) use or disclosure in connection with legal proceedings; or

(d) use or disclosure reasonably believed to be necessary to avert an imminent threat of serious violence to any Person or substantial damage to property.

For example, use or disclosure of Computer Surveillance records can occur in circumstances of assault, suspected assault, theft or suspected theft of Council's property (or that of a related corporation of Council) or damage to Council's equipment or facilities (or that of a related corporation of Council).

5.9 Use of Financial Accounting Systems

(a) Access to Council's Financial Accounting System will be limited to authorised personnel only. Unauthorised access is strictly prohibited.

(b) Users of the Accounting System shall not disable, enable or interfere with software settings designed to improve security.

(c) Users should protect their Accounting system username and password information at all times and not divulge such information to any other person.

(d) Accounting System Users must not use another User's password or username to log in to the Accounting System for any reason.

(e) Accounting System users must change their passwords at least once every quarter to ensure security against unauthorised system access.

(f) The Finance Manager is responsible for ensuring appropriate user access and permissions.

(g) Permissions and access to the Accounting System will be reviewed by the Finance Manager and updated as required.

5.10 Enforcement

Users must comply with the requirements of this policy. Any breach of this policy may result in disciplinary action which may include termination of employment (or, for Persons other than employees, the termination or non-renewal of contractual arrangements).

Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to all or part of Council's Computer Network whether permanently or on a temporary basis.

Users may also be subject to criminal charges if they are in breach of policy

Examples of Policy breach include but are not limited to:

(a) Any unauthorised interception, reading, copying or modifying of electronic data on Council's computer systems;

(b) Unauthorised access to other persons electronic files, emails, records management system, accounting system, or other electronic communication system;

(c) Any attempt to break password protected files whether successful or not;

(d) Any communication intended to bring Council or its officers into disrepute; and

(e) Any attempt to circumvent user authentication or security of any host network or account.

6. Review of Policy

This policy will be reviewed when any of the following occur:

1. The related documents are amended or replaced.
2. Other circumstances as determined from time to time by a resolution of Council.

Notwithstanding the above, this policy is to be reviewed at intervals of no more than three (3) years.

7. Key Responsibilities

Position	**Responsibility**
Mayor	To lead councillors in their understanding of, and compliance with, this policy.
CEO	To lead staff (either directly or through delegated authority) in their understanding of, and compliance with, this policy.
Directors	To communicate, implement and comply with this policy.
Managers and Supervisors	To implement this policy and related procedures.
All Council staff	To comply with this policy and consider its implications for related projects and programs.

8. Related Documents

- *Australian Copyright Act 1968* - proscribes the copying of software or data files (including text, sound and images) in the absence of a licensing arrangement;
- *Crimes Act 1914* - describes procedures related to dealing with a crime;
- *Cybercrime Act 2001* - deals with a range of computer related offences;
- *Privacy Act 1988* - introduces principles related to protection of personal information; and
- *SPAM Act 2003* – which proscribes the sending of SPAM messages.
- *Crime and Corruption Act 2001* - establishes a commission to reduce the incidence of corruption in the public sector. Council must preserve and make information available for this Commission so that it can be effective in its investigations;
- *Copyright Act 1968* - is an Act relating to copyright law;
- *Criminal Code Act 1995* - proscribes computer hacking and general misuse;
- *Electronic Transactions (Queensland) Act 2001* - refers to the integrity of information and requirements to keep information associated with the need for businesses and the community to use electronic communications when dealing with government bodies;
- *Evidence Act 1977* - defines what must be preserved as evidence related to government activities;
- *Information Privacy Act 2009* - ensures the security and protection of personal information and restricts the collection, use and disclosure of information about an individual;
- *Right to Information Act 2009* - makes particular types of information concerning government documents available to members of the community in order to ensure such information is timely and accurate;
- *Local Government Act 2009* - requires local government employees not to wilfully destroy or damage Council records;
- *Public Records Act 2002* - states the responsibilities of government in the management of corporate records - particularly with regards to security; and
- *Public Sector Ethics Act 1994* - states the responsibilities public officials have in ensuring that public resources are not wasted, abused or improperly used.
- Burke Shire Council Code of Conduct
- Burke Shire Council Portables and Attractive Items Policy
- Burke Shire Council Fraud Policy
- Burke Shire Council Social Media Policy
- Burke Shire Council Strategic ICT Management Framework