Blackall-Tambo
Regional Council

Computer, Email and Internet Policy

30 September 2016

Policy Number: Admin 6
Version Number: Two

Chief Executive Officer

C D Blanch

Mayor

Cr Andrew Martin

....

....

Table of Contents

Computer, Email & Internet Usage Policy

1 RESOLUTION

05/09A/16

2 PURPOSE

Blackall-Tambo Regional Council (BTRC) is a highly computerised organisation with various software programs being used to undertake core functions of Council. The Internet is recognised by government and business organisations as a serious and valuable information resource. It provides information on a wide variety of subjects that may be useful to council staff and Councillors. Computer access includes access to external electronic mail (email) for all staff and Councillors or other authorised persons with a PC login ID and access to the World Wide Web (WWW).

This document describes the access methods, services available and user and management responsibilities when using computers within Council. Staff and Councillors who have access to the internet have an obligation to use their access in a responsible and informed way. Managers and supervisors have a responsibility to ensure the internet is used appropriately by staff under their control.

All Council policies, procedures and requirements with regard to ethical behaviour, fraud, risk management and records management apply to the use of the internet and email. In addition, the provisions of the *Local Government Act 1993* regarding the use and confidentiality of Council information, apply to all staff and Councillors.

3 DEFINITIONS

3.1 "PRIVATE USE"

The term "private use" refers to the personal or unofficial use of council resources and includes anything that is not directly related to the work you do for BTRC. It excludes any personal use provisions contained in individual contracts of employment.

3.2 "RESOURCES"

The term "resources" refers to **anything** owned, controlled or paid for by the Council regardless of its state of repair or future use within the organisation. This includes, but is not limited to:

3.2.1 Physical Resources such as:

- Equipment e.g. Computer equipment, software, power tools, machinery, cameras, motor vehicles, fuel, spare parts and accessories, office equipment and stationery, consumable materials used in a process, off-cut materials
- Surplus materials that have been costed but not used on a project
- Waste products able to be recycled

- Recyclable materials and items – including metals
- Packaging and storage items
- Materials subject to deterioration, which are regularly replaced to maintain safety or quality standards
- Perishable items that have exceeded their used by date
- Items deemed to be obsolete due to advances in new technology
- Items in good condition, but deemed unusable due to circumstance
- Damaged, inefficient or non-working items considered to be uneconomical to repair
- Seconds produced as part of a process
- Items of low value that are not controlled by the asset register
- Assets originally of high value that have diminished in value over time

3.2.2 Intellectual Resources such as:

- Council correspondence, reports or records (other than those documents on the public record).

3.2.3 Financial Resources such as:

- Petty cash, purchase orders, purchasing identification cards

3.2.4 People Resources such as:

- An employees work time or the work time of others

3.2.5 Natural Resources such as:

- Water, trees, shrubs, seedlings and flowers

4 ABBREVIATIONS

WWW   –   World Wide Web

BTRC   –   Blackall-Tambo Regional Council

PC   –   Personal Computer

ID   –   Identification Document

IT   –   Information Technology

ITO   –   Information Technology Officer

Email   –   Electronic Mail

HRO   –   Human Resource Officer

5 APPLICATION

5.1 THIS POLICY APPLIES TO:

a) Any persons, whether a permanent, temporary, contracted or casual employee of BTRC who has access to BTRC Information Technology (IT) resources.
b) All guest/visitors of the BTRC

c) Any other authorised Users or organisations accessing BTRC IT resources

5.2 COMPUTER SOFTWARE AND HARDWARE AND PROCEDURES

Council provides computer software and hardware to enable Councillors and staff to perform their various functions within Council.

5.2.1 Software

All software installed on Council computers (desktops or notebooks) must have valid licences. Council is liable for any illegal software installed on computers. Harsh penalties exist for organisations that install and use illegal software.

Information Technology Officer (ITO) must be notified and licences verified prior to the installation of any software on Council computers (software includes programs, screen savers, utilities etc.). Personal software shall not be installed on Council computers.

ITO regularly undertakes audits for inclusion in the Software Registration database. Illegal software will be uninstalled and departmental managers notified.

5.2.2 Hardware

Computer hardware is defined as computer (desktop or notebook) equipment and attached peripherals including keyboard, mouse, printer etc.

Staff and Councillors are responsible for the good care of computers and equipment. Faults or problems shall be reported to ITO as soon as practical. Devices and peripherals shall not be connected without the approval of ITO.

ITO regularly undertakes audits and checks for inclusion in the Hardware Registration Database.

5.2.3 Electronic Mail

Electronic mail (email) is an electronic message sent by one person to another person who has Internet mail access. The email service provided can be used for sending email messages to external organisations and within Council.

All electronic files should be presumed to be the property of Council. Immediacy of transmission does not always translate into immediacy of receipt. Where a response is required immediately or the matter is urgent, it might be advisable to consider using other means of communication.

Messages that concern matters of policy and official communication between Council and other organisations should be emailed to or printed and forwarded to Records for entry into the records management system.

5.2.4 Message Formats

E-mail can be one of two formats, either informal or formal.

Informal email can be defined as brief messages that do not relate to the business of the sender or recipient. There is no necessity for either the sender

or recipient to view such informal communications as an official Council record.

Formal email, however, should be viewed as an official Council record and should be constructed accordingly, using appropriate file references and staff designations. The sender or receiver, in accordance with records management procedures, should forward a copy to the records department.

Documentation may be subject to Freedom of Information and Judicial Review, and therefore, individual staff are responsible for anything they write.

5.3   ACCEPTABLE USE AND EMAIL ETIQUETTE

Staff should remember that body language, facial expressions and vocal inflections DO NOT travel with e-mail messages and be aware in composing messages, that their contents have the potential to be misconstrued by the recipient. When sending email:

- Act in a professional and courteous manner. Be discreet in what you send. Avoid gossip. Statements about others may find their way back to them. Avoid sarcasm.
- Use mixed case in email messages. DO NOT use uppercase only.
- Always proof read and spell check messages before sending them.
- Keep your email messages brief and to the point. DO NOT clutter other people's email accounts with unnecessary messages.

Practice good "house-keeping" by:

- Checking email daily.
- Deleting unwanted messages immediately.
- Keeping messages remaining in electronic mailboxes to a minimum.
- Downloading or extracting to private folders on your "C Drive", mail messages required for future reference.

Refrain from unacceptable practices, including:

- Publicising or sharing your password in any way.
- Using somebody else's account.
- Using your account or the facilities and capabilities of the internet to conduct any business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group or list members to use goods or services.
- Council staff must be completely impartial when sending emails to commercial businesses in the Region. There must not be any suggestion that a Council officer being the sender of an email is favouring, promoting or endorsing one business over another.
- Publishing on or over the network any information that violates or infringes upon the rights of any other person, or any information of an abusive or profane nature, or material likely to be sexually offensive to an average person. (No Information should be published that infringes on State or Commonwealth *Anti-Discrimination Acts.*)
- Using offensive, discriminatory or defamatory language. (There are laws relating to written communication that apply equally to e-mail

messages, including those for defamation, racial discrimination, fraud, sexual harassment, copyright and obscenity.)

- Using your account for political lobbying.
- Using your account to harass another person.
- Seeking or gaining unauthorised access to any resource or entity.
- Using your account for criminal purposes or for any illegal purposes or activity, including violation of copyright or other contracts.
- Invading the privacy of other individuals.
- Using your account to send anonymous messages defined either as messages that do not contain details of your name and affiliation, or messages sent through an anonymous re-mailing service.
- Vandalising the data of another user. (Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or any agencies or other networks connected to the Internet.) This includes, but is not limited to, the uploading or creation of computer viruses.
- Posting to a discussion group or other public forum, personal communications without the author's consent.
- The sending of chain letters to groups or individuals and any other type of use which would cause congestion of the network or otherwise interfere with the work of others.
- Reading or attempting to modify e-mail belonging to others.
- Misrepresenting the Council.

Established procedures regarding the signing of official correspondence also apply to email. Staff should NOT forward any official correspondence via email without their Manager's approval.

All care should be taken to ensure that external email messages are addressed correctly.

It should be noted that the e-mail system is a communication tool provided by Council to carry out Council business (not personal business). Professional ethics and common sense require that personal messages be kept to a minimum. Personal email messages by staff and Councillors are to be confined to "out of work hours".

Council will install email-monitoring software. Initially the software will be configured to monitor and report on email usage. Attachments will be screened to prevent viruses corrupting Council hardware and software. Image files including JPEG, GIF, AVI etc will be quarantined and their suitability assessed before being forwarded.

Care should be taken when forwarding emails. The sender's permission may be required to be obtained prior to the message being forwarded.

5.4 PROCEDURES FOR THE USE OF EMAIL

1. Email should be treated with the same significance as the signed letter. The ability for you to send an email message has the same authority as signed correspondence.

2. All emails shall have the authorise signature block which is approved by council which is that in the Email Signature section.
3. Email must be accessed at least once a day by each employee with access to a networked personal computer. Any unwanted email should be deleted.
4. Staff can maintain their own email address book.
5. Personal or private information such as personal notes or invitations, staff appraisals or job applications should not be included in an email message because it could be read by, or misdirected to, unauthorised persons. Messages may also continue to exist long after the sender has deleted them. Deletion eliminates the message or file name from your computer directory but the information itself exists in the back up system until it has been overwritten.
6. Remember that email is admissible as evidence in court so use good judgment and think carefully about what you write.
7. Make sure you follow email etiquette.

5.5 EMAIL SIGNATURES

This standard email template must be used by all staff and this template have been provided for:

a) Internal memos
b) External correspondence

Regards
Your Name
Job Title

P: (07) 4621 6600
F: (07) 46** ****
M: 04** *** *** (make line blank if no mob phone)
E: ****@btrc.qld.gov.au

Blackall-Tambo
Regional Council

Exploring the past. Innovating the future.

****

Blackall-Tambo Regional Council – Confidential communication

This email and any files transmitted with it are confidential and are intended solely for the use of the addressee. If you are not the intended recipient be advised that you have received this email in error and that any use, dissemination, forwarding, printing or copying of this email and any file attachments is strictly prohibited. If you have received this email in error, please immediately notify us. You must destroy the original transmission and its contents.

****

Please think of the environment before printing this email. Thanks

5.6 FILE TRANSFERS

The transfer of files across the internet affects the performance of the Council computer network. It is important to realise that the bigger a file is, the longer

it takes to transmit across the network and the more *bandwidth is* required. This can have a major effect on all other systems running on the network.

In order to avoid network congestion a **maximum file size of 5.5mb** has been determined and the firewall software will not permit files larger than this size to come in to or go out of the Council network.

A degree of caution should be exercised when sending files with email messages, to ensure that confidential or unrelated files are not inadvertently sent.

5.7 DISCLAIMER

The following Disclaimer shall be use when sending external email messages:

****

Blackall-Tambo Regional Council – Confidential communication

This email and any files transmitted with it are confidential and are intended solely for the use of the addressee. If you are not the intended recipient be advised that you have received this email in error and that any use, dissemination, forwarding, printing or copying of this email and any file attachments is strictly prohibited. If you have received this email in error, please immediately notify us. You must destroy the original transmission and its contents.

This Disclaimer is the same as that in the [Signature Section](#)

5.8 CONTRACTS

The use of email as a means of communicating contractual correspondence is NOT ACCEPTABLE unless the "contract" itself contains a clause or section specifically accepting email for such purpose. The acceptance of "contract documents", as being valid, when transmitted via email is always subject to the conditions of the contract itself.

5.9 EMAIL ADDRESSES FOR COUNCIL STAFF

Email addresses for individuals will be that of their job position, followed by Council's registered *domain name,* for example: ceo@btrc.qld.gov.au. This email will only be with the individual while in their current position and will be transferred to whoever takes over that job position

Council's general address for all other email is: admin@btrc.qld.gov.au.

Email addresses **are NOT case sensitive**, however, spacing and punctuation should be observed when using email addresses to ensure they are correct prior to transmission.

5.10 INTERNET (WORLD WIDE WEB)

Outlined below are the conditions under which use of the internet has been provided.

The internet must only be used to carry out official duties and contribute to the accomplishment of Council goals. Unauthorised use of the internet is not permitted.

5.11 UNAUTHORISED USE

Examples of unauthorised use are:

The use of or access to the internet for inappropriate use or obscene or illegal activities or in support of such activities.

Inappropriate use shall be defined as the violation of the intended use of the internet or use of the internet for other than the purpose and goals of Council.

Obscene activities shall be defined as a violation of generally accepted social standards.

Illegal activities shall be defined as a violation of State, Commonwealth or International laws.

Staff who have NOT been granted access to the internet through their own login ID should NOT attempt access via another login ID, unless directed to do so by their department Manager.

5.12 UNETHICAL OR UNACCEPTABLE ACTIONS

Any activity that is unethical and unacceptable would be just cause for taking action. This may include formal disciplinary measures, depending on the offence. Unacceptable action may include but is not limited to the following:

- Violation of institutional or third party copyright, licence agreements or other contracts (refer also to the section on copyright in this document).
- Interference with the intended use of the information resources (internet).
- Seeking to gain unauthorised access to information resources ie breaking into unauthorised networks like NASA or ATO.

Using or knowingly allowing another to use your internet account to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises, or representations.

Without authorisation destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer-based information and/or information resources.

Without authorisation invade the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources transmit or cause to be transmitted communications that may be construed as harassment or disparagement of others based on the criteria of *Anti-Discrimination* legislation and Council policy.

Violate any laws pertaining to the unauthorised use of computing resources or computer networks.

Conducting any activity on the internet that is in breach of the BTRC Code of Conduct for Employees and Councillors.

5.13 MISUSE

It is the responsibility of Managers and Supervisors to ensure that staff under their control are using their computer and internet correctly. It is also the

responsibility of each individual user to ensure that they have control over their computer and internet access and keep secure their login password.

When expressing views on the internet through email or forums, it is important that *this* be in accordance with the BTRC Code of Conduct for Employees and Councillors

Internet usage will be monitored and details of users accessing prohibited web sites, obtained and forwarded to the appropriate manager for consideration. Prohibited web sites are those that contain inappropriate or obscene information as outlined in *this* document

Staff must ensure that any information or opinions obtained via the internet be independently validated, as they are generally provided with no responsibility held by the originator and /or provider.

5.14 DOWNLOADING FILES

Strict rules apply to the downloading of files from external sources, including email and the internet.

5.15 GAMES

No game will be downloaded from the Internet onto any Council machine.

5.16 OFFENSIVE MATERIAL

Pornographic or other material of an offensive nature is NOT to be searched for or downloaded. This restriction includes such material in textural, graphic and image format.

Staff and Councillors are advised that *Content Checking* software will be installed to quarantine such material and bring this event to the attention of the CEO. Persons attempting to access offensive web sites can easily be identified by their login ID.

Responsibility for internet usage is associated with your user ID and is similar to that used for speed cameras or parking infringements where the registered owner of a vehicle, not necessarily the driver, incurs the penalty for illegal activities.

5.17 EXECUTABLE FILES AND PROGRAMS

No computer programs or executable (.exe) files are to be downloaded onto any Council computer without permission of the ITO, and approval from your Manager or Supervisor.

5.18 SECURITY

Email is not always a secure medium, particularly when sent via the internet.

Email, along with other parts of the Council computer network, is regularly "backed up" and may therefore be preserved for some period of time on back-up tapes.

Anyone who in the course of their work has access to records, files, or data belonging to others should take reasonable precautions to avoid invading the privacy of individuals without their knowledge, and should not divulge or

disclose such information to others, unless required by Council policy or State or Commonwealth Law.

Security is essential for the effective and efficient operation of the internet and for the provision of services and is the responsibility of all users.

Security on any computer system is a high priority. If you feel you can identify a security problem on the internet, notify the ITO immediately – **do not** demonstrate the problem to other users.

5.19 LOGIN PASSWORDS

You are responsible for any email sent, files viewed or sites visited via your username or login. It is therefore important to maintain security of your login password. Select only passwords that are not easy to guess or founded by simple password-cracking program.

It'll be set up that you'll have to adhere to the password guidelines. Passwords also will be set so they will be required to be changed every 6 weeks. This will be enforced via a policy on the server.

The following guidelines are provided to assist staff in selecting and safeguarding appropriate passwords:

- Do not use words that can be found in the dictionary;
- Do not use birthdays, pay or employee numbers, position numbers, addresses or any other identification code that might be easily guessed or found in other information about yourself;
- A combination of 6 or more letters (both uppercase and lowercase), numbers and symbols, or some of these should be selected;
- Keep your password confidential and do not write it down;
- When leaving your computer unattended, please remember to log off or lock your workstation, so that any other staff member cannot use your email account in your absence.

Responsibility for internet usage is associated with your user ID and is similar to that used for speed cameras or parking infringements where the registered owner of a vehicle, not necessarily the driver, incurs the penalty for illegal activities.

5.20 RESPONSIBILITIES

Staff must not give their password to another staff member or member of the public and must not access other staff members email without appropriate authority. Unauthorised access to programs or information will result in disciplinary action.

Each User is responsible for:
- The unique computer accounts which BTRC has authorised for the User's benefit. These accounts are not transferable.
- Selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer or locking the computer.
- Familiarising themselves with legislative requirements which apply to the use of IT resources and acting accordingly. To the extent allowed

by law, BTRC takes no responsibility for Users whose actions breach Federal or Queensland legislation.

5.21 ILLEGAL INTRUSIONS

As an account holder you should immediately notify the ITO if you have forgotten your password, had it stolen, or have reason to believe that someone has obtained unauthorised access to your account

The internet has the potential for illegal intrusions and email accounts are particularly vulnerable to break-in. All suspected violations should be treated seriously.

If you suspect your account has been tampered with, change your password immediately and contact the ITO with specific details.

Clues to determining unauthorised access may include:

- Strange files appearing in a directory;
- The system reporting a login when you weren't using your computer;
- Files or programs changing size or no longer functioning properly.

Council will implement content checking (text scanning) and tracking software as part of its internet connections and services.

These software programs detect viruses and prohibit inappropriate information from being exported or imported via email or the internet. Such items, when detected, are automatically quarantined from the Council network and the ITO is notified.

Content checking software will open encapsulated and zipped files of any format. Council staff should be aware that serious consequences would result if inappropriate material were detected being exported from or introduced to the Council network.

5.22 VIRUSES

It is important to be aware that some email messages may arrive with file attachments and that there are risks involved when downloading files from unknown sources.

Regardless of any virus protection measures that have been installed, it is always possible that newer virus strains may be able to penetrate virus scanning at the firewall or the desktop.

When forwarding files you should maintain a record of whom you are sending it to and where these files are distributed in case there is a virus infestation. This will make it easier to contain the situation if this did occur. All downloaded data will be automatically scanned at *point of entry to* the network.

5.23 ACCESS AND AVAILABILITY

Access to email is available at all times to all staff through their normal login privileges. Mail is delivered and sent using Microsoft Outlook (Exchange Server). Access to the internet is available via Microsoft Internet Explorer and is restricted to staff who have a User ID.

A program will be set up to disallow people going to certain sites during work hours (eg. Ebay, facebook, Twitter).

It is the Human Resource Officer's (HRO) responsibility to inform the ITO of any new staff who will be starting that will need to have computer, email and internet access. This shall be done 1-2 weeks before their official starting date so as the ITO can have the username, user password and email address back to the HRO in time by the starting date.

5.24 USER SUPPORT

User support for technical difficulties ONLY, will be available from ITO during normal Council working hours *(Monday to Friday - 8.22am – 4.45pm).*

5.25 TRAINING SUPPORT

Help for MS Outlook is available from within Outlook or by contacting the ITO. Other users in your section may be able to assist with minor problems.

5.26 COPYRIGHT AND LICENSING

Copyright law applies to all material published on the Internet. You are responsible for complying with all copyright use and restrictions where noted on web documents. It is important to locate and read all copyright notices. Keep the following guidelines in mind:

- Search for copyright notices regarding any material you intended to use;
- Always seek permission before copying, redistributing, or editing any copyright material;
- Comply with any licenses or permissions that grant the right to redistribute or otherwise use any copyright material;
- Always include a copyright notice with any such material if the copyright owner (ie. material courtesy of) requires it.

5.27 COUNCIL "WEBSITE"

Responsibility for the Council website and home page is shared between the ITO and selected staff members.

The address for this website is: www.btrc.qld.gov.au

6 SECURITY OF INFORMATION TECHNOLOGY (IT) RESOURCES AND DATA

6.1 AUTHORISED USER'S RESPONSIBILITIES

Users have a responsibility at all times to:
- Act lawfully.
- Keep all BTRC IT resources secure and to observe the BTRC's policy.
- Not compromise or attempt to compromise the security of any IT resource belonging to BTRC or other organisations or individuals, nor exploit or attempt to exploit any security deficiency.
- Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power

management, anti-static measures, protection from theft, and sound magnetic media practices.

- Ensure their computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

6.2 CONFIDENTIAL INFORMATION

Authorised Users have a duty to keep confidential:

- All BTRC's data unless the information has been approved for external publication.
- Information provided in confidence to BTRC by other entities.

Each staff member is bound by an obligation to not disclose BTRC's business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

6.3 RESPONSIBILITY FOR GUIDELINES

These guidelines were approved by Council on 21 September 2016.

Amendments to these guidelines may only be made through written advice to the following contact officer:

User Contact: Chief Executive Offier

Authority for change approval:

Chief Executive Officer

Your Manager should first approve requests for amendments.

Approved: ……………………………..

Name: C D Blanch

Position: *Chief Executive Officer*

Date:

7 USER DECLARATION FORM

Declaration of IT User Policy Acceptance

User Details:

Family Name:_____

Other Names:_____

Position:_____

Phone:_____ Fax:_____

Email:_____

User Declaration - Conditions of Use:

- I understand that the information I will have access to is confidential and must not be shared or divulged to any unauthorised person.
- I will use only those IT facilities for which I have been authorised.
- I understand that IT facilities may only be used for the purposes for which they have been provided and are not to be used for other projects, games, 'hobby computing', or private or consulting work (unless authorised).
- I understand that IT facilities must not be wasted or consumed by inappropriate or irresponsible use.
- I must not attempt to tamper with any IT facility in any way which might alter or impede its use by others.
- I must not harass or offend others, including using computing facilities to send unlawful, obscene, abusive, offensive, fraudulent, threatening or unnecessarily repetitive messages.
- I will take every reasonable precaution to ensure that passwords, accounts and data are adequately secured.
- Any computer account allocated to me is for my exclusive use. I will not allow another person to use it without the authorisation of my manager.
- I agree to comply at all times with the IT User Policy.

I understand and agree to the above Conditions of Use.

SIGNATURE: …………………………………………………………………

PRINT NAME: …………………………………………………………………

DATE: …………………………………………………………………………..

8 CHANGES SINCE LAST REVISION

New Policy as of 27 January 2010 to reflect current procedures.

Revised 30 September 2016 to prevent favouring, promoting, or endorsing one business over another.

9 RECORDS

When completed and approved the original, signed hard copy of the policy is filed in the Master File.

Electronic copies are saved in the appropriately labelled folder in InfoXpert.