BLAND SHIRE COUNCIL
west wyalong

POLICY STATEMENT

INTERNET, EMAIL & COMPUTER USAGE

POLICY ADOPTED: **19 March 2014**

---

1. Policy Objective:

The objective of this policy statement is to provide Council employees with clear guidelines for the use of internet, e-mail and computer usage to allow for effective communication between employees and others with whom Council communicates.

Staff will be required to sign-off on this policy at the commencement of their employment to certify that they understand and agree to comply with the terms of this policy.

Council has given its employees access to telecommunications, e-mail, computer, internet and other facilities to assist them to communicate effectively with each other and others with whom Council communicates, and to use the information gathering and storage capabilities that the facilities provide. Council also recognises that occasionally, employees may wish to use the facilities for private purposes, to meet family and community responsibilities.

2. Policy Statement:

The unique nature of internet, e-mail and computer facilities is supported by this policy which has the purpose of:

- Preserving the integrity and efficiency of the facilities by providing guidelines for employees to clarify what constitutes appropriate conduct and use of the facilities;
- Outlining the expectations Council has of the manner in which employees will use the facilities, so that they enhance the professional and personal lives of employees, while complying with the organisation's obligations to maintain a workplace that is efficient, harmonious and without risk of discrimination or harassment resulting from improper use of the facilities; and
- Outlining to employees what will happen if they fail to abide by the guidelines contained in this policy.

3. Definitions:

Council means Bland Shire Council

Computer Equipment means and includes any electronic equipment or computer software, provided to employees for use in the performance of their duties, either in general or specific terms, including, but not limited to:

- Computers, including PC's, laptops/notebooks, tablets and handheld devices;
- Printers;
- Scanners;
- Digital cameras or any other digital imaging equipment;
- All software and programs provided to facilitate work needs;
- Network operating systems (eg Windows 2000);
- All network infrastructure including data cabling and transmission equipment;
- All forms of e-mail including use of webmail.
- Internet access
- Mobile phones connected to the internet and/or email.

Council's Record Management Procedures incorporates Policies, Procedures or Protocols in place from time to time which determine how business records are received, stored, actioned and referred throughout the organisation. Refer to "Records Management" policy.

Employee means and includes all persons engaged, whether on a permanent, temporary, seconded or contract basis as well as contractors engaged to work for or on behalf of the Council including elected members of the Council.

Normal Working Duties means and includes all activities associated with fulfilling the duties and obligations of the Employee's Position Description.

Privileges means and includes the specific permission granted to access and/or use Computer Equipment including areas where electronic files may be stored, modified or viewed and the quality of such storage space which will be made available.

Streaming means Multimedia (audio and video) files that start to play in a steady and continuous flow, almost immediately upon their downloading.

Work Related Study means and includes study and research approved by an employee's relevant Director for the purpose of developing skills required in the performance of their position.

Social Media means a group of Internet-based applications that build on the ideological and technological foundations that allow the creation and exchange of user-generated content. Furthermore, social media depend on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content.

Authorised Officer means and includes the following positions:

- General Manager
- Director of Corporate, Community & Development Services
- Director of Assets & Engineering Services
- Manager Development Services
- Corporate Services Coordinator
- Manager Finance

- Manager of Library and Children's Services
- Manager Works

4. **Responsibilities:**

This policy applies to all Bland Shire Council employees, Councillors, work experience students and volunteers.

5. Recommended Practices:

5.1 Use of facilities

Council has provided the facilities primarily for business purpose and to enhance the productivity and quality of work. Private use of facilities should be restricted to breaks.

5.2 Legal issues

Council and its employees may be legally liable if the facilities are used in an unlawful way. The following legislation is relevant:

a. NSW Anti-Discrimination Act 1977;
b. NSW Privacy and Personal Information Protection Act 1998;
c. NSW State Records Act 1998;
d. Evidence Act 1995;
e. Federal Sex Discrimination Act 1984;
f. Federal Disability Discrimination Act 1992;
g. Federal Racial Discrimination Act 1975;
h. Federal Crimes Act 1900;
i. Federal Copyright Act 1968;
j. Federal Defamation Act 1974;
k. Defamation Act 2005 (NSW);
l. Employees Liability Act 1991 (NSW); and
m. Crimes Act 1914 (Cth).

The guidelines in this policy are based upon the requirements of this legislation, so as to protect both Council and its employees from legal action.

5.3 Authorisation of Use

Employees of the Council will be granted privileges to use computer equipment supplied by the Council, following confirmation of their employment and the required authorisation forms being completed by an authorised officer.

6. System Security

6.1 Responsibility of Director in consultation with Councils IT contractors

It is the responsibility of the Director in consultation with Councils IT contractors to provide, maintain and monitor the necessary hardware and software (eg Anti-Virus) to minimise security risks.

6.2 Passwords

It is the responsibility of each employee to maintain the confidentiality and security of their own password. Employees should ensure that they:

a. Log off the network or password lock their workstation whenever leaving it unattended for long periods of time, including attending meetings and lunch breaks;
b. Do not attempt to gain access to another employee's log-in id or password; and

c. Do not disclose passwords to any other persons.

Persons who are not employed by Council must not be given access to the Council's corporate network under any circumstances, unless approval is first sought and obtained from an Authorised Officer. This includes work experience students, volunteers, etc. Where approval to access equipment and software is conditionally given, such persons are not permitted to use an existing user's log-in id or password. In such circumstances, an authorised officer will arrange a temporary account with the appropriate security privileges.

6.3 Communications System Security

To help avoid the spread of viruses, employees must not by-pass Council's network security by accessing the internet directly by modem or other unauthorised means, unless permission has been granted by an authorised officer.

Employees using IT equipment with access to Council's network and not utilising Council supplied IT equipment, must ensure that any file or data brought into Council from an external (to Council) source, is scanned with Council approved virus checking software. The Director of Corporate, Community and Development Services must be notified immediately, if any employee suspects that a virus has been introduced into Council.

6.4 Hardware, Software and Privileges

Employees must not attempt to install or remove software or hardware onto Council's Computer Network without prior approval and direction from an authorised officer.

Streaming: Streaming material via Council's network utilises bandwidth and slows network performance. Therefore, no network users are permitted to "stream".

As a requirement of the State Records Act, all Council information and/or data is to be permanently stored on Council's servers for backup and security implications. Therefore, disk space on individual Council PC's or Council laptops, should only be used as temporary storage, or for transitional purposes only. Please note that in general, Council PC's or Council laptops are not backed up in any way.

Employees must not attempt to access, copy, damage, delete, insert or alter any information held on Council's Computer Equipment beyond the Privileges granted by an Authorised Officer for the performance of their normal working duties.

7. E-mail usage

7.1 Privacy

E-mail is made available to Council Employees primarily to enable Council to conduct its business communications efficiently. All e-mails sent or received from Council's system remain the property of Council. For legal purposes, e-mail has the same standing in court as paper documents.

Employees should not expect that e-mail is confidential or private. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful

consideration should be given as to whether alternative means of communication are preferable.

Whilst Council does not wish to become a censor, to ensure that the guidelines contained in this policy are followed, council retains the right to access or view users' e-mail sent via the corporate network. Council will only access information created or stored on Council's e-mail system for disciplinary procedures or where there is a valid business requirement.

7.2 Management of e-mail messages

E-mail is a valid form of communication within Council. Employees should attempt to access their e-mail at least once per day. Employees must manage their e-mail mailbox personally by ensuring that e-mails received are actioned within acceptable times, unwanted e-mails are cleared, and business communications are registered in accordance with the State Records Act of 1998, e-mail messages are official records of Council's business and the legislation requires Council to be accountable for that business. Transactions that provide evidence of business activities, which include but are not necessarily limited to:

a. What happened;
b. What was decided;
c. What advice was given;
d. Who was involved;
e. When it happened; and
f. Order of events and decisions.

are required to be documented in the Records Management System to provide an official record.

E-mail messages that document such activities, should be forwarded electronically to Records for registration into the Council Records Management System.

When employees go on leave, it will be their responsibility to ensure that arrangements have been put in place while they are on leave, so that their e-mails can still be processed or acknowledged in some way.

7.3 Standards for Outbound E-mail

The content of e-mail signature files is to clearly state the identity of the e-mail originator. Employees should include their name, title, telephone number, e-mail address and Council website address above a high resolution image of Council's logo on all e-mails.

Example:

BLAND SHIRE COUNCIL
west wyalong

John Citizen
BSC Employee
PO Box 21
West Wyalong NSW 2671
Ph: 02 6972 2266

Fax: 02 6972 2145
jcitizen@blandshire.nsw.gov.au
www.blandshire.nsw.gov.au

7.4 Acceptable personal use of e-mail

Council accepts that e-mail may on occasion be used for personal reasons. Acceptable personal use includes sending short personal e-mails preferably during lunch breaks or outside normal work hours. However, employees must remember that the primary purpose of the e-mail system is to enhance business communication and hence, the overall effectiveness of the organisation. Excessive personal use of the e-mail can undermine that effectiveness and lead to disciplinary action.

7.5 Unacceptable use of e-mail

Employees must not access, or attempt to access, another employee's e-mail while in transmission or stored on a system without authorisation from the employee whose e-mail is to be accessed, or an authorised officer. Any e-mails caught by virus cleaning software will no longer be considered private and will be open for interrogation by the General Manager, Directors or an Authorised Officer. Employees specifically must not use e-mail (including personal e-mail) to:

a. Conduct illegal activities;
b. Send e-mail messages that in any way could, or would be likely to bring Council's name into disrepute;
c. Send e-mail messages (with or without attachments) which contain inappropriate or offensive material of a sexual, racial, libellous, defamatory, abusive, obscene or discriminatory nature;
d. Distribute "junk mail" or electronic chain letters including letters seeking donations and those providing pyramid selling schemes or advertising;
e. Send unauthorised e-mails from another person's e-mail address or impersonating another person;
f. Send e-mails which are likely to be perceived as harassment, intimidation or an unwanted invasion of privacy;
g. Send non-urgent e-mails (e.g. jokes) to large numbers of people (whether within Council or not) at any time; and
h. Send personal e-mail to any person who does not wish to receive it. If a recipient asks a user to stop sending him or her e-mail, their request must be observed.

7.6 What you should do if you receive offensive e-mail

If an employee receives offensive e-mail from outside Council, they should immediately delete. In the event that further material is received, the employee should advise their supervisor.

7.7 Limitations

Council has implemented a maximum size for allowable e-mail messages and also restricts e-mail messages that contain certain attachments or content which have been known to contain viruses from either entering or leaving Council. Users will be notified by (return) e-mail, when such limits have has been exceeded. An authorised officer should be contacted on a case by case basis, if these limitations are found to be too restrictive.

8. Internet Usage

8.1 Access to sites

Employees should be aware that internet sites accessed by them can record Council's name. Council can monitor sites that employees are accessing and it reserves the right to do so, to ensure that the guidelines contained in this policy are followed.

Council reserves the right to block access to sites which it deems to be inappropriate.

8.2 Sending information

The internet is not a secure method of sending information. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

8.3 Acceptable personal use of internet facilities

Council accepts that the internet facilities may on occasion be used for personal use reasons. Acceptable personal use includes browsing the internet during lunch breaks or outside normal work hours. However, employees must remember that the primary purpose of the internet facilities is to enhance business activities and hence, the overall effectiveness of the organisation. Excessive personal use of the internet facilities can undermine that effectiveness.

8.4 Unacceptable use of internet facilities

Employees specifically must not use the internet facilities to:

a. Intentionally access sites which contain pornography, or inappropriate or offensive material of a sexual, racial or discriminatory nature;
b. Solicit, download, store, or distribute pornography, inappropriate or offensive material of sexual, racial or discriminatory nature;
c. Access internet chat clients or internet relay chat networks;
d. Conduct gambling activities;
e. Conduct private transactions of a personal gain/profit nature, either directly or indirectly;
f. Conduct gaming activities during working hours; and
g. Stream music or programs as these activities utilise significant bandwidth and has a detrimental effect on Council's activities.

9. Social Media

Bland Shire Council recognises that social media provides new opportunities for dynamic and interactive two-way communication which can complement existing communication and further improve information, access and delivery of key services.

When establishing a social media account on behalf of Council, users must complete the Social Media Account Checklist (Appendix A) and submit to the relevant Director for approval and the General Manager for authorisation.

For further information regarding social media, please refer to Bland Shire Council's Social Media Policy.

10. iTunes/Android Accounts

Bland Shire Council recognises that to fully utilise technology available, the creation of an iTunes/Android account may be required.

When establishing an iTunes/Android account on behalf of Council, users must complete the iTunes/Android Account Checklist (Appendix B) and submit to the relevant Director for approval and the General Manager for authorisation.

All log in details and passwords must be supplied to records and stored in Council's Record Management System in a confidential folder.

11. Personal Use – General

11.1 Acceptable Personal Use

Notwithstanding the concessions made for acceptable personal use of e-mail and internet facilities in Sections 7.2 and 7.4, Council accepts that its Computer Equipment may on occasion be used for personal use reasons. Acceptable personal use includes the following, conducted during lunch breaks or outside normal work hours and consistent with all other sections of this policy:

a. The creation and storage of personal computer files, up to a total of 100 Megabytes at any one time, and which must be stored only in the section allocated for personal files on Council's Corporate Network; and
b. The limited use of printers with the verbal (or written) agreement of an authorised officer.

However, employees must remember that the primary purpose of Council's computer equipment is as a tool for business and hence, to enhance the overall effectiveness of the organisation. The provision and maintenance of computer equipment and consumables is a cost to Council's business activities and therefore excessive personal use of these facilities can undermine the effectiveness of the organisation.

Employees must not use Council's computer equipment to maintain or support a personal business activity under any circumstances.

11.2 Work Related Study Use

Use of Council's computer equipment, including e-mail and internet, may be granted to an individual staff member for work related study purposes by agreement with an authorised officer.

This agreement must:

a. Be consistent with all sections of this policy.

The agreement may:

a. Be for a fixed period;
b. Contain limits on the equipment available for use;
c. Contain limits on the time periods when study use may take place;
d. Require that records of use are to be maintained;
e. Detail the apportionment of costs associated with the usage; and
f. Permit variation by mutual agreement at any time.

Agreements for Work Related Study Use may be revoked at any time by an authorised officer by written or verbal notification to the employee.

12. Copyright:

All employees must respect the copyright and any other intellectual property rights of third parties.

Copyright protects the exclusive right of the copyright holder to copy, publish, perform, broadcast and sell copyrighted material. Employees must not download material from the internet or otherwise receive and use information that is owned by a third party unless they have the written permission of that party.

Examples of possible breaches of copyright can include forwarding e-mails or copying or downloading copyright material (including computer programs, screensavers, sounds and images) that have copyright protection.

As a general rule, under copyright law downloading from the internet for personal research is allowed. However, downloading material for distribution to others or for business purposes will require the permission of the third party owner.

13. Other Issues

13.1 Workplace Health and Safety

It is the responsibility of Council to ensure:

a. Employees are aware of any relevant issues pertaining to the correct handling and usage of computer hardware and software; and
b. That monitors meet current Australian safety standards.

Employees must ensure:

a. That all cabling is arranged tidily so as not to present a health or operational hazard; and
b. That equipment is used in accordance with guidelines of this and other Policies and Procedures as may be adopted from time to time.

13.2 Education and Training

It is the responsibility of supervisors to ensure employees are made aware of the contents and purpose of this policy, and compliance requirements of the policy.

13.3 Monitoring and Auditing of Equipment, Services and Software

Employees must be aware that:

a. Computer usage, including internet access and e-mail, will be monitored to ensure that the guidelines contained in this policy are followed. This includes monitoring personal usage of computer equipment during and out of normal work hours;
b. Logs may be kept indicating internet sites employees have visited; and
c. Authorised officers may request such monitoring to take place with respect to an employee for which they are responsible, and may view such monitoring or logs as are available.

14. Compliance with Policy:

14.1 Read the policy

All employees must read this policy carefully and observe its requirements. It is the employee's responsibility to ensure that they understand their obligations in relation to the policy.

Employees must also sign the attached acknowledgement of understanding form prior to being granted access (or continuing access) to the facilities. Employees must not sign unless they fully understand and agree to comply with all the terms of this policy.

14.2 Conditions of employment

Compliance with this policy is a condition of each employee's employment with Council. A breach of any part of this policy may, depending on the circumstances, be regarded as a serious breach of any employee's employment contract with Council.

14.3 Breaches of the policy

A failure to comply with this policy and any relevant directions given by management may result in the following action being taken against an employee:

a. Counselling (including intensive training on this policy and the appropriate use of facilities); and/or
b. Disciplinary action regarding "inappropriate use" of the facilities, including cancellation of access to any or all of the facilities; and/or
c. Dismissal in cases such as the access and/or distribution of material outlined in the unacceptable use of e-mail or unacceptable use of internet facilities sections of this policy.

15. Variations:

The policies and procedures at Bland Shire Council are the management tool developed to assist in operational requirements. This policy may be reviewed, varied or revoked according to these requirements. No change will take effect until it has been appropriately communicated to employees.

16. Internet Disclaimer:

Upon accessing the internet via the Council's network, you immediately release, discharge and indemnify Council of all liability and responsibility;

a. With respect to defamatory or other offensive material that you may access on the internet by reason of web searching and browsing by you;
b. Relating to any costs incurred associated with the use of on-line shopping services or any monetary transaction undertaken by the employee not directly relating to Council business;
c. With respect to the unauthorised use of copyrighted material obtained via the internet.

17. Commitment:

Councillors and staff are required to initially commit to this policy by signing this document to acknowledge that they have read the policy and agree to comply with its terms.

18. References:

- NSW Anti-Discrimination Act 1977;

- NSW Privacy and Personal Information Protection Act 1998;
- NSW State Records Act 1998;
- Evidence Act 1995;
- Federal Sex Discrimination Act 1984;
- Federal Disability Discrimination Act 1992;
- Federal Racial Discrimination Act 1975;
- Federal Crimes Act 1900;
- Federal Copyright Act 1968;
- Federal Defamation Act 1974;
- Defamation Act 2005 (NSW);
- Employees Liability Act 1991 (NSW); and
- Crimes Act 1914 (Cth).
- Bland Shire Council Code of Conduct
- Bland Shire Council Communications Policy
- Bland Shire Council Social Media Policy and Procedure

19. Appendices:

Appendix A – Social Media Account Checklist
Appendix B – iTunes/Android Account Checklist

20. Authorisation:

Status	**Committee**	N/A	
	Manex	19 March 2014	
Owner	**Director Corporate Community & Development Services**		
EDRMS Doc. ID	405218		
Superceded Policy			
Date of Adoption/ Amendment	**Revision Number**	**Minute Number**	**Review Date**
17 August 2004	0	15/8/04	September 2008
19 March 2014	1		March 2015

Related Council Policy / Procedure

Appendix A

Social Media Account Checklist

The following checklist is a good place to begin when considering setting up a social media account and determining its purpose.

1. What will our account name be?

- Can we get a name that aligns with our organisation-services?
- Can we get a name that matches other social media accounts we already have?
- All Council pages must commence with “Bland Shire” followed by the position or department title (eg Bland Shire Mayor) or a position or department title followed by “Bland Shire” (eg General Manger Bland Shire).
- All Council social media pages are owned by Bland Shire Council.

2. What email account will it be linked to?

- Can this email be accessed by multiple staff or one person only?
- If it is a corporate account will it block communication from the site?

3. Who can post/publish items to the account?

- Will publishing responsibility be restricted to an individual or team of people?
- How will the messages be controlled, fact checked, spell checked?
- Is it important that any communications have a similar ‘voice’ or style?
- Will this be officially recognised as part of people’s work plans with time allocated to the activity? If so, how much time?

4. What type of content can be published?

- What will the account be used for primarily?
- Will we post images or just text?
- Will we post details of events/promotions for organisations outside of Council that we are not a partner with, or attending?
- Will we post details of events/promotions for other areas of Council?
- What about activities/groups that staff are involved with outside of work?
- What is our policy about naming staff members online?
- What do we do with information that may be critical of Council or politically sensitive e.g. new development application?

5. Who is our target audience?

- How will we reach them?
- Why are we doing this?

6. Who/what will we follow/friend or NOT?

- Will we follow official Council accounts from our own Council?
- Will we follow other Councils?
- Will we follow local media?
- Will we follow Councillors?
- Will we follow individual members of staff?
- Will we follow members of the public?
- Will we follow political parties?
- What about legal service providers, businesses, emergency services, Government organisations, community groups, lobby groups, clubs etc.?

7. Who/what will we block and why?

- What is our legal/moral obligation here?
- Will we block illegal, offensive, defamatory material? Political/fundraising material?
- Advertising/promotional material?

8. Will we Direct Message followers/friends?

- Will our communication/posting be public? – remember many of our followers/friends may be under 18 years of age.

9. How will we track/monitor our postings/communication?

- Will we use a third party product?
- What will our policy be about deleting posts?
- Should copies be kept of deleted posts?
- Do we need to archive posts? How often? How?

Appendix B

iTunes/Android Account Checklist

The following checklist is a good place to begin when considering setting up an iTunes/Android account and determining its purpose.

1. **What will our account name be?**
   - Can we get a name that aligns with our organisation-services?

2. **What email account will it be linked to?**
   - Can this email be accessed by multiple staff or one person only?
   - If it is a corporate account will it block communication from the site?

3. **What type of content can be purchased?**
   - What will the account be used for primarily?

4. **How will we track/monitor our purchases?**
   - Will we use a third party product?

5. **What devices will purchases be downloaded to?**
   - They will be available to all devices linked to the itunes account (maximum of five devices).

6. **What payment details will be used on the account?**
   - A Bland Shire Council credit card will be required to set up an itunes account, permission and credit card details will be supplied by the relevant Director.