INTERNET, EMAIL AND COMPUTER USE POLICY

Approval Date: 13 April 2011

Review Date: 5 June 2019

Responsible Officer: Director of Corporate & Urban Services

1. PURPOSE

This policy sets out the standards of behaviour expected of persons using Coonamble Shire Council's ('**Council**') computer facilities, networks or when making reference to Council on external sites including social networking sites, as well as standards required when accessing and using confidential or sensitive information that Council may hold.

This policy also sets out the type of surveillance that will be carried out in Council's workplace, relating to the use of Council's Computer Network.

This policy applies to all people who use Council's Computer Network by any means (***Users***), including employees, contract staff, volunteers, work experience placements and any other person. The policy also applies to Users who contribute to external blogs and sites including social networking sites who identify themselves as being associated with Council.

This policy does not form part of any employee's contract of employment. Nor does it form part of any other User's contract for service.

2. DEFINITIONS

'***Blogging***' means the act of using web log or 'blog'. 'Blog' is an abbreviated version of 'weblog' which is a term used to describe websites that maintain an ongoing chronicle of information. A blog is a frequently updated website featuring diary-style commentary, audio-visual material and links to articles on other websites.

'***Confidential Information***' includes but is not limited to trade secrets of Council; non-public information about the organisation and affairs of the Council such as: pricing information such as internal cost and pricing rates; marketing or strategy plans; commercial and business plans; contractual arrangements with third parties; tender policies and arrangements; financial information and data; training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from Council or obtained in the course of working or providing services to Council that is by its nature confidential.

'***Computer Surveillance***' means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of Council's Computer Network (including, but not limited to, the sending and receipt of emails, text messages and the accessing of websites).

'***Computer Network***' includes all Council's internet, email hand held device and computer facilities which are used by Users, inside and outside working hours, in the workplace of Council or at any other place while performing work for Council. It includes, but is not limited to, desktop computers, laptop computers, portable devices with internet access including smart phones and similar products, and any other means of accessing Council's email, internet and computer facilities, (including, but not limited to, a personal home computer which has remote access to Council's IT systems).

'***Intellectual Property***' means all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name, and all Confidential Information and including know-how and trade secrets.

'***Person***' includes any natural person, company, partnership, association, trust, business, or other organisation or entity of any description and a Person's legal personal representative(s), successors, assigns or substitutes.

'Social networking / media site' means a web-based or group of web-based application(s) that enables the creation and exchange of user-generated content. Social media can occur in a variety of formats including chat rooms, weblogs, and social blogs. Examples of social networking sites include, but not limited to LinkedIn, YouTube, Flickr, Facebook, Twitter, MySpace, YouTube and other similar sites.

3. POLICY STATEMENT

3.1 USE OF INTERNET, EMAIL AND COMPUTERS

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

Users are permitted to use Council's Computer Network for limited and reasonable personal use. 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.

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.

3.2 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 should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.

d) Users should ensure that when not in use or unattended, the computer/device is logged off or shut down.

e) A disclaimer is automatically included in all Council emails, and must not be removed.

f) 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 the IT Department for assistance.

g) If a User receives an email, text message or other electronic message where 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 the Director of Corporate & Urban Services. The User must not forward the email or text message to any other person, unless for the purpose of forwarding to the investigator.

3.3 PROHIBITED CONDUCT

Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email, text message or electronic 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) or in a text message or as an attachment to a text message. For example, material of a sexual nature, indecent or pornographic material;

b) 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;

c) is considered bullying and harassment in line with Council's Bullying and Harassment in the Workplace Policy

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.

g) Further, Users must not transmit or send Council's documents or emails or text messages (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) in a manner contrary to Council's privacy policy;

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

d) to disclose any confidential information of Council or any customer, rate payer, client or supplier of Council's unless expressly authorised by Council;

e) 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;

f) 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;

g) to send or cause to be sent chain or SPAM emails or text messages in any format;

h) to use Council computer facilities for personal gain. For example, running a personal business.

Users must not use another User's Computer Network facilities (including passwords and usernames/login codes) for any reason without the express permission of the User's supervisor or Director.

Users must not wilfully delete or password-protect electronic information and files, including emails, which could be constituted as a malicious act or to prevent Council easy access to that information.

3.4 DETAILS ON BLOCKING EMAIL OR INTERNET ACCESS

Council reserves the right to prevent (or cause to be prevented) the delivery of an email or text message sent to or from a User, or access to an internet website (including a social networking site) by a User, if the content of the email, text message 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), or in or attached to a text message. 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 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's Computer Network, or internal or external communications in any way;

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.

3.4 CONFIDENTIAL / SENSITIVE INFORMATION

In the course of conducting Council business, Users may have access to confidential, personal or commercially sensitive information.

Users must:

a) Users must consider the sensitivity of information and not use information contrary to Council's Code of Conduct and privacy legislation.
b) Not disclose confidential / commercially sensitive information to any unauthorised person.
c) Immediately declare if access to information creates, or could be perceived to create, a conflict of interest.
d) Take all steps to prevent unauthorised access or use of this information
a) Comply with any reasonable instruction may by Council or of a related corporation of Council.

Users may be asked to sign additional agreements related to access to confidential / sensitive electronic information, especially if related to software and electronic databases of a related corporation of the Council (i.e. RMS).

3.5 TYPE OF SURVEILLANCE IN THE 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);
f) computer hard drives – Council may access any hard drive on the Computer Network;
g) text messages – Council may access any text messages stored on a User's hand held device and the User must provide Council with the device for the purpose of allowing such access; and
h) mobile telephone records – Council may access the records of a User's hand held device that has been provided by Council.

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 alleged misconduct.

3.6 WHAT WILL THE COMPUTER SURVEILLANCE RECORDS BE USED FOR?

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, the retention of any other User 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 or other injury to any person or substantial damage to property.

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

3.7 SOCIAL NETWORK SITE

Council's Facebook page includes social networking facilities that only authorised Users may use.

Authorised Users are only permitted to contribute to comments and social network entries in order to share information and knowledge, obtain constructive feedback, interact directly with rate payers' clients, collaborate over projects and solve problems, promote the organisation, and raise Council's profile.

Only Users who are authorised by the Director of Corporate & Urban Services are permitted to publish a blog or social network entry on any sites operated by Council, and the content of any such blog or entry must first be approved by Director of Corporate & Urban Services before publishing.

3.8 STANDARDS IN RELATION TO BLOGS AND SITES NOT OPERATED BY THE COUNCIL

Council acknowledges that Users have the right to contribute content to public communications on websites not operated by Council, such as social networking sites like Facebook, Twitter, YouTube and others. However, inappropriate use of such communications has the potential to cause damage to Council, employees, clients and suppliers. For that reason, the following provisions apply to all Users:

a) As it may not be possible for any user of an external site to conduct a search that will identify any blogged comments about Council, Users must **not** publish any material which identifies themselves as being associated with Council.

b) Users must not publish any material that may expose Council to any possible legal liability. Examples include, but are not limited to, defamation or discrimination proceedings.

c) Users should be aware information placed on social media/networking sites, such as Facebook, may easily be forwarded on to a third party. It is the responsibility of the User to understand how the social media/networking site they are accessing operates.

Apart from the potentially damaging effects a blog or social networking entry may have on Council, inappropriate blogs on internal or external sites can also have adverse consequences for a User in terms of future career prospects, as the material remains widely and permanently accessible to other site users.

There is no such thing as a 'private' social media/networking site. Posting information on-line is a public activity.

3.9 BREACH OF THIS POLICY

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 non-renewal of contractual arrangements in serious cases. Other disciplinary action that may be taken includes, but is not limited to, formal written warnings, suspension or disconnection of access to all or part of Council's Computer Network whether permanently or on a temporary basis.

4. RELATED DOCUMENTS AND LEGISLATIVE PROVISIONS

- Local Government Act 1993
- Model Code of Conduct for Local Councils in NSW
- Coonamble Shire Council Publication Guide
- Model Privacy Management Plan
- Private and Personal Information Protection Act 1998 (NSW)
- Private and Personal Information Protection Regulation Act 2005 (NSW)
- Workplace Surveillance Act 2005
- Social media policy ??

5. POLICY REVIEW

As this document is an internal operational policy, it will not be submitted for approval at Council meetings. This policy may be amended or revoked at any time and must be reviewed at least two (2) years since its adoption (or latest amendment).

Policy Review History

Date	Changes Made	Approved By
13 April 2011	Policy developed and authorised	General Manager
5 June 2017	Policy reviewed, amendments made and authorised	General Manager

Policy Adopted and in effect on: 13 April 2011

RICK WARREN
GENERAL MANAGER

INTERNET, EMAIL AND COMPUTER USE POLICY

I acknowledge and agree to the following:

1) I have received a copy of Council's Internet, Email and Computer Use Policy
2) I have read and understood the contents of the Policy
3) I will comply with the contents of the Policy
4) I am aware that a breach of this Policy may lead to disciplinary consequences, including termination of employment.
5) I am aware that Council monitors the use and content of electronic information accessed on Council's Computer Network, including internet, email and portable devices.

Name: _____

Signed: _____

Date: _____