

## 1 Policy History

Revision No.	Council Meeting Date	Minute No.	Adoption Date
1	15/10/2002	851	15/10/2002
2	14/01/2003	25	14/01/2003
3	14/03/2006	92	14/03/2006
4	11/05/2010	0142	11/05/2010
5	27/01/2015	15/005	27/01/2015
6	13/02/2018	18/046	16/03/2018

## 2 Policy Objective

- To provide internal procedures to be followed by Council staff relating to use of email services including the creation, access, transmission, retention and management of email and use of internet facilities provided by Council.
- To make all Council employees aware of Council's Email and Internet policy.
- To ensure that Council's computer system is used in the most efficient manner.
- To ensure that all of Council's business emails are preserved as required by the NSW State Records Act and its amendments.

## 3 Policy Statement

### 3.1 Scope

This policy covers all incoming and outgoing email messages received and transmitted via Council's computer network. The grant of internet access and use of email to Council employees is not a right but is subject to and conditional upon compliance with this Email and Internet policy. Email messages and their attachments are taken to be corporate records if they serve to document Council's business. Generally speaking emails should be captured into the corporate recordkeeping system when they:

- Approve or authorise actions
- Constitute formal communication between staff
- Signify a policy change or development
- Relate to significant projects or activities being carried out
- Contain advice or provide guidance
- Constitute formal communication between staff and individuals outside the organisation
- Have value in support of a project or activity being carried out by the organisation.

### 3.2 Cyber Bullying

Cyber bullying involves the use of electronic communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others.

**Electronic communications can encompass:**

- Email
- Short Message Service (SMS)
- Multimedia Message Service (MMS)
- Social media networking/photo sharing websites, blogs and chat rooms.

Electronic communication activity produces a 'digital footprint' that is difficult to remove, is not controllable and may resurface as evidence at any time.

**Work place cyber bullying may be identified to have occurred when it can be established:**

- There is a relationship to a role or individual at Council
- The bullying has been conducted during Council time or by using Council resources
- An event or incident can be linked to having occurred during Council time

**Specific examples of cyber bullying can include but are not limited to:**

- Malicious or threatening emails or SMS communications
- Electronic communication which features offensive content such as profane language or explicit images
- Electronic content that promotes, fosters or perpetuates discrimination related to gender, ethnicity, disability, religion or sexual preference
- Distribution of embarrassing, offensive or manipulated images or videos of an individual

Acts of cyber bullying are breach of the Workplace Bullying Policy (HR-PO-213) and Code of Conduct (GC-CP-404).

### 3.3 Email Policies

- a) The email system is part of Council's computer network. All information processed, transmitted or stored is the property of council. There is no such thing as a private e-mail on council's system. Council staff are permitted to use Council's email system for personal use provided that such use is reasonable as determined by the General Manager. Personal use of email is a privilege and not an automatic right and may be withdrawn at any time at the discretion of the General Manager.

- b) Any attempt to access Council's computer network remotely or providing assistance to any other person to gain such access, for example from an individual home computer without the express authorisation of the IT Manager may be grounds for disciplinary action in accordance with the Local Government Award.
- c) The primary purpose of the Council's email system is to conduct Council business.
- d) Users must not use email for any unlawful purpose. Council also reserves the right to report any illegal activities carried out using the Internet to the appropriate authorities.
- e) Access to email is restricted to Council staff, Councillors and other authorised persons, who have been given a user identification and password.
- f) Staff must not give their password to any other person and must not access other staff members email without appropriate authority. Such conduct may be grounds for disciplinary action in accordance with the Local Government Award and may be grounds for dismissal.
- g) Users must not download any attachments containing executable files, graphics, games, software (including multimedia software), images, videos or audio files unless this is for a business related purpose which has been approved by the IT Manager. When sending emails, Council employees should avoid attaching unnecessary graphics. Council employees should also ensure that any attached files are checked before being forwarded to the addressee to ensure that the correct document is attached.
- h) Email etiquette should be followed. Keep messages polite and do not use emotive, abusive or obscene language. Do not mark messages "High Priority" unless they are truly urgent.
- i) All authorised Council Internet and email users are reminded that the Anti-Discrimination Act 1977 (NSW) and Council's Equal Employment Opportunity policies must be complied with. Authorised users shall not send or distribute emails or Internet material which is offensive or inappropriate. Emails must not contain inappropriate language such as expletives or prohibited content. Prohibited content includes but is not limited to religious, racist, sexual or sexist comments or jokes, pornography, references to illicit drugs, sex, sexual preferences, the commission of a crime, politics or religion.
- j) Where an authorised user of Council's email system receives an offensive or inappropriate email from an external source, he/she should immediately forward any such email to Council's email administrator (usually the IT Support Officer) who will ensure that appropriate action is taken.

- k) Council's General Manager reserves the right to request that the IT Department provide a list of all email addresses contacted and to view the contents of any emails sent or received via Council's computer system by any authorised user. If the General Manager makes such a request the authorised user affected may be notified in writing by the General Manager.

### **3.3.1 Legal Obligations**

- a) For legal purposes, email has the same standing in court as paper documents. Users must ensure that emails do not contain any content that may bring Council into disrepute or expose Council to legal action. Email is the equivalent of a signed letter.
- b) An authorised user of Council's email system and Internet facilities is prohibited from entering into any on-line contract on Council's behalf or binding Council in any manner whatsoever except with the express authority of the General Manager and nothing in this Email and Internet Policy will be construed as conferring any such right on an authorised user.

### **3.3.2 Security**

- a) The security and privacy of email transmissions cannot be assured. Council staff must be aware of the potential risks involved in sending personal or sensitive information by email. For this reason personal or sensitive information should not be included in emails (or attachments) as they can be intercepted, read by or sent to unauthorised recipients. In all cases, staff members must ensure that appropriate security is provided to protect communication from unauthorised use, publication or alteration. Any issues that the user is unable to resolve must be drawn to the attention of that user's manager. If appropriate, staff members should seek advice from Council's IT Department prior to sending any information of a confidential/sensitive nature via the Internet.
- b) Messages continue to exist long after the sender has deleted them. Deletion eliminates the message or file name from the user's computer directory, but the information itself exists in the backup system until it has been overwritten. The sender of email must be aware that control of e-mail is lost once it has been received by another party, that is, email could be forwarded to other recipients without the knowledge of the original sender.

### **3.3.3 Privacy and Email Monitoring**

- a) Council employees are issued with a user ID and password to protect email against unauthorised access.

- b) However, Council reserves the right to monitor all incoming and outgoing emails received or transmitted via Council's computer system to ensure that Council's Email and Internet policy is being adhered to.
- c) Council reserves the right to copy and archive all incoming and outgoing email. Such archives will be kept for a minimum of 2 months. Emails that have been deleted at the user's terminal may have been backed up and are recoverable by Council's IT Department.
- d) Council may review and block any incoming or outgoing email messages using its "Mail Marshal" software which is designed to scan content and attachments and where appropriate to block access to certain types of attachments containing questionable material.
- e) The current settings in Mail Marshal block the following types of attachments:
  - File size greater than 10 Mb
  - Executable files (.exe, .com etc)
  - Image files (.gif, .jpg etc)
  - Video **or Sound** files (.mpeg, .wav etc)
  - Viruses
  - Unknown or suspect attachments
  - Unacceptable language
- f) Blocked emails that are positively identified as being work-related will be scanned for viruses and if clear will be released.
- g) Council reserves the right to change its email filtering application and the above settings from time to time.
- h) Council's IT Department may generate monthly reports as well as on a random basis to determine the extent and nature of email use by individual users. Reports will contain the number of, and addresses, of all emails sent and received by individual users.
- i) If a Council employee is identified as using his/her email account for non-business related purposes, except as permitted under clause xviii that individual's account may be suspended or revoked and notification sent to his/her manager. In such circumstances, the account will only be reinstated at the direction of the manager to whom the individual reports to or the General Manager.

#### **3.3.4 Standard Disclaimer**

- a) Mail Marshal stamps all outgoing emails with a standard disclaimer to protect Council and to remind recipients of their security and privacy obligations regarding the circulation of email.

- b) The following message is currently attached to all outgoing email.

This e-mail, together with any attachments, is for the exclusive and confidential use of the addressee(s). Confidentiality is not waived if you are not the intended recipient. Any other distribution, use of, or reproduction without prior written consent is strictly prohibited. Views expressed in this e-mail are those of the individual, except where specifically stated otherwise. If this e-mail has been sent to you in error, please delete the e-mail completely and immediately from your system. Although reasonable precautions are taken, Griffith City Council does not warrant or guarantee this message to be free of errors, interference, viruses or similar malicious code and does not accept liability for any consequences to the recipient opening or using this email or attachments.

This email was scanned and cleared by Trustwave MailMarshal,  
Sophos & Kaspersky AV

### **3.3.5 Housekeeping**

Quotas are not set on email accounts. Employees are required to perform regular housekeeping practices to ensure compliance with the NSW State Records Act.

- a) Every Council employee should ensure that his/her emails are reviewed at a minimum, twice daily. Any messages which are no longer required should be deleted from that employee's Inbox and the Sent Items and Deleted Items folders.

- b) It is the responsibility of the user to manage documents in these folders.

It is recommended that email be regularly deleted or saved into Council's corporate records management system.

- c) For extended periods of leave, arrangements for the handling of email should be made.

Please discuss any concerns you may have with Council's IT Department.

## **3.4 Email Procedures**

### **3.4.1 Corporate Records**

- a) Staff sending and receiving email are responsible for deciding if an email message is considered to be a Council corporate record. If a staff member is unsure as to whether an email message is a corporate record, he/she should consult the manager to whom that individual reports. Emails identified as corporate information are required to be captured into the corporate recordkeeping system. An internally

generated email is to be captured by the creator before distribution. An email received from external sources is to be captured into the records management system by the first receiver.

- b) Email messages that become part of Council corporate records must be retained in accordance with the approved retention periods listed in the Local Government Disposal Schedule.

### **3.4.2 Email Address**

- a) Email can be sent internally and externally using IBM Notes. Council reserves the right to change this application from time to time. Any mail sent to the organisation electronically should be addressed to Council's official address, [admin@griffith.nsw.gov.au](mailto:admin@griffith.nsw.gov.au). This address is the equivalent of Council's PO Box and accordingly will be controlled and maintained by Council's Corporate Information Section. Individual Officers are also able to receive email via a personal email address. An email address is a combination of the user's name and Council's external email address. Each user inserts their name at the beginning of the email address to create a unique email address that directs email to their personal mailbox.

Email address format: [firstname.surname@griffith.nsw.gov.au](mailto:firstname.surname@griffith.nsw.gov.au)

Example: The email address for John Smith would be:  
[john.smith@griffith.nsw.gov.au](mailto:john.smith@griffith.nsw.gov.au)

### **3.4.3 Training**

- a) Training on the use of IBM Notes is available by contacting the Workforce Planning Manager and is included with new staff induction training.

## **3.5 Internet Policies**

Internet access will be given to individuals at the discretion of their manager or the General Manager. Staff may apply to their manager requesting Internet access. Internet access is subject to the following policies:

- a) An authorised user must not use the Internet for any unlawful purpose. Council also reserves the right to report any illegal activities carried out using the Internet to the appropriate authorities.
- b) An authorised user must not attempt to access a website that falls into a category that is classified by Council as prohibited.

Such categories include but are not limited to pornography, gambling and chat rooms, and other sites reasonably determined by the General Manager as being prohibited. If an authorised user accesses a site that falls into the



prohibited category, this may be grounds for disciplinary action in accordance with the Local Government Award.

- c) Access to the Internet is granted to Council staff for the primary purpose of conducting Council business. However, Council staff are permitted to access the Internet for personal use provided that staff do not access websites classified by Council as prohibited or unauthorised except with the consent of the General Manager. In addition, Council staff must not use the Internet for any unlawful purpose and any use of the Internet must be reasonable as determined by the General Manager. Access to the Internet is a privilege and not an automatic right and may be withdrawn at any time at the discretion of the General Manager.
- d) All sites accessed will be registered against the individual user as well as time spent on each site. Council uses a time tracker against sites accessed. Data downloaded from any sites may be made available to the General Manager for review.
- e) Any attempt to access Council's computer network remotely or providing assistance to any other person to gain such access, for example from an individual home computer without the express authorisation of the IT Manager will be grounds for disciplinary action in accordance with the Local Government Award.
- f) Council reserves the right to and will monitor all Internet access on Council's computer system. There is no such thing as private internet access on Council's computer system.
- g) Council reserves the right to block access to any net address (URL) that it considers inappropriate.

### **3.5.1 Internet Monitoring**

- a) Council's internet management system Web Marshal has been designed to record all internet transactions and to report on all sites visited and by whom. Reports will be generated monthly as well as on a random basis to determine the extent and nature by Internet use of individual users.
- b) The current settings in WebMarshal block and monitor the following types of Web sites.
  - Webmail
  - Offensive language
  - Gambling
  - Pornography
  - Non business sites



- c) Training to facilitate the most productive methods of retrieving data from the Internet can be provided by the IT Department on request.
- d) All sites accessed will be registered against the individual user as well as time spent on each site. Council uses a time tracker against sites accessed, which will determine whether or not the site has been accessed during or after work time.
- e) Data downloaded from any sites after hours may be made available to the General Manager for review. If an authorised user of the Internet is subject to any access restrictions during normal business hours, these will apply after hours.

### 3.6 Policy Review

This policy will be periodically reviewed as required to take into account any legal requirements and technological advances.

### 3.7 Fundamental Term of Employment Contract

It is a fundamental term of all Council employees' employment contracts that all Council employees comply with this Email and Internet policy. Use of Council's email services and Internet facilities will be taken to be acceptance of this policy and of the conditions of your employment contract. Further, access will only be maintained where this policy and the terms of your contract of employment are accepted by replying to the administrator's email message which will be issued on providing access. A copy of the acknowledgment will be placed on the employment file as evidence of you having read and accepted Council's Email and Internet policy. Failure to provide an acknowledgment within 24 hours of receipt will result in the facilities being withdrawn.

I, \_\_\_\_\_ (name)

Hereby accept the terms and conditions of this Email and Internet Policy dated.....

Signed: \_\_\_\_\_

Dated: \_\_\_\_\_

## 4 Definitions

None

## 5 Exceptions

None

## 6 Legislation

NSW State Records Act  
Local Government State Award 2014  
Anti-Discrimination Act 1997 (NSW)

## 7 Related Documents

Workplace Bullying (HR-PO-213)  
Equal Employment Opportunity – EEO (HR-PO-231)  
Council's Code of Conduct (GC-CP-404)

## 8 Directorate

Economic and Organisational Development



I, \_\_\_\_\_ (name)

Hereby accept the terms and conditions of this Email and Internet Policy dated.....

Signed: \_\_\_\_\_

Dated: \_\_\_\_\_