



**INTERNET, EMAIL AND MOBILE  
COMPUTING POLICY**

## Amendments

Date	Amendment	Reference
1 May 2012	Adopted	CS/19

## **Applicability**

This policy applies to all authorised users using Council equipment who have access to the Internet and/or email.

## **Policy Statement**

Council provides email and Internet facilities to staff and authorised users to undertake Council related business. The Internet and email system has been developed to support Council's business function and enhance communication.

Council will allow reasonable personal use of its email systems and authorised users are encouraged to use good judgement and integrity when they do so, however the Council provided email should not be the users' primary personal email service. Personal messages should not interfere with the business function or processes of Council and should not be used for purposes that are expressly prohibited.

The Internet can be used for personal reasons outside of work hours provided it is not used for reasons expressly prohibited by Council and that usage is intermittent and not regular. The accessing of websites that are not directly related to the completion of Council business inside of work hours is not permitted.

Email messages are legally recognised in the same way as letters and memorandum. As a consequence, spontaneously written email messages may provide evidence in litigation for or against the individual or Council. For this reason, users must not impart anything in an email message that he or she would not be comfortable saying in a public forum and for which they may be held accountable.

Council embraces social media as an important tool to engage in conversations with its own community, and recognises the need to have a policy which ensures that users who use social media either as part of their job, or in a personal capacity, have guidance as to the Council's expectations where the social media engagement is about Council, its services, its people and or other business related individuals or organisations. When engaging in social media users must be clear about who they are representing, that they take responsibility for ensuring that any references to Council are factually correct and accurate and do not breach confidentiality and that they show respect for the individuals and communities with which they interact.

It is important to note that this policy does not apply to personal use of the Internet, Email, Mobile Devices and Social Networking outside of Council's premises and/or Council provided computing facilities, providing the user makes no reference when doing so to Council, its services or its people.

## **General Principles**

1. Council provided Internet (Intranet) and email privileges, like Council computer systems and networks, are considered Council resources and are intended to be used for business purposes only. Usage and content is monitored and this may be reported to Management in the event of unusual activity or content.
2. As a general guide, use email like you would the phone. Messages are to adhere to this policy. They are to be kept short, and graphics used only where it is absolutely essential to convey communication about the topic or issue at question. Only attach or discuss information that you know is approved or publicly accessible. If in doubt, talk to your supervisor or the Manager IT Services.

3. All email messages are scanned for viruses, and if detected they will not be allowed to leave or enter the organisation.
4. As a general rule any unsolicited email containing attachments or hyperlinks should be considered suspicious. If in doubt IT Services should be contacted before accessing, opening, replying or forwarding of any suspicious email.
5. Correspondence via email is not private. Authorised users should have no reasonable expectation of privacy in the use of the email and internet services as Council may be required to copy, access or disclose any information or files that are stored, processed or transmitted using Council equipment.
6. Any correspondence via email is considered a Corporate Record of Council and must be retained in accordance with the State Records Act.
7. Authorised users are required to ensure that where appropriate, electronic copies of email(s) received are registered into Council's Document Management System (DataWorks) as prescribed by the State Records Act for retention.
8. Council email accounts, Internet IDs and Web pages should not be used for anything other than Council-sanctioned communications.
9. Internet/Intranet and email resources may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
10. The distribution of any information through the Internet, computer-based services, email and messaging systems is subject to the scrutiny of Council management. Council reserves the right to determine the suitability of this information.
11. All email messages; incoming and outgoing are recorded, and could be viewed by authorised personnel under delegated authority from the General Manager at any time.
12. An Employee's email account may be accessed at any time by the relevant employee's Manager, Director and/or the General Manager where necessary and with regard to the conducting of Council business processes or procedures. This will also apply to Contractors provided with a Council email address.
13. A Councillor's Council provided email account may be accessed at any time by the General Manager or the Public Officer where it is deemed necessary under the Code of Conduct and/or to ensure records of Council business are retained as required by the State Records Act and/or Government Information (Public Access) Act.
14. Internet usage must be able to survive public scrutiny and/or disclosure. Users must avoid accessing sites that may bring the Council into disrepute, such as those, which carry offensive material. Sensitive information must not be transmitted via or exposed to Internet access.
15. Usage of the email system must be able to survive public scrutiny and/or disclosure. Users must not use the email system to:
  - promote a personal business or commercial gain
  - send, receive or access illegal, hostile, fraudulent, slanderous, obscene, pornographic, offensive, profane or erotic material
  - violate copyright
  - distribute confidential, sensitive or private personal information as legislated by the Government Information (Public Access) Act or the Privacy and Personal Information Protection Act
  - send, receive or access non-work related video, sound or photographic files
  - send, receive or access chain letters, hoaxes, junk mail and/or other SPAM classed correspondence

- send, receive or access information and/or data files to which a fee may apply, unless that fee has been paid
16. Authorised users may use Internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not used for personal financial gain.
  17. Internet sites such Social Networking sites (including but not limited to Facebook and Twitter), Internet Forums, Message Boards, Chat rooms or Blogs may be used only to conduct work related business where this has been clearly identified within the staff members position description and/or annual workplan or has been specifically authorised by their manager or director. Users who wish to express personal opinions on Social Networking sites, Internet Forums, Message Boards, Chat rooms or Blogs must use a private Internet provider and a personal ID.
  18. If or when using the Internet to access Social Networking Sites and/or Email Services in a personal capacity, and reference is given to Mosman Council, its employees or Councillors in any post, email or comment, the user must clearly indicate that the views or opinions stated are their own and do not represent those of Mosman Council.
  19. If or when using the Internet to access Social Networking Site(s) in any capacity as authorised above, you must ensure that any content you publish is factually accurate and complies with Council policies (including but not limited to this policy), and particularly those relating to confidentiality and disclosure.
  20. Staff and contractors should not have work related clients as friends on their personal social network accounts.
  21. The IT Services section must ensure that all users sign an Internet Usage Agreement (attached) before access is allowed. This agreement is now incorporated into existing system access agreements.
  22. The IT Services section monitors the use of the Council network. Information incoming and outgoing via the Internet or Email will be scrutinised at any time by the IT Services Section under delegated authority from General Manager. Alleged inappropriate use of the Internet will be reviewed by the Manager IT Services on a case by case basis and referred to the appropriate Manager for disciplinary action to be taken in accordance with the policy, up to and including dismissal or cancellation of contract.
  23. Emails are automatically scanned for viruses, compliance to policy, SPAM and other potentially offensive content. Messages are automatically blocked or passed based upon a set of criteria defined within the tool. The system in place will notify staff of blocked messages, except where they are classified as containing a virus, are potentially offensive or are classified as SPAM, Spyware or Malware.
  24. Staff members are to be reminded that details such as credit card numbers and passwords may be intercepted on the internet and/or in emails, or within the Council environment as part of regular monitoring of electronic communications.

## **Sanctions & Breach of Policy**

Users who violate any of the guidelines and conditions of use of this policy will be a breach of the general conduct obligations under Council's Code of Conduct and may be subject to disciplinary action including (but not limited to) written warnings and revocation of access privileges or, in serious cases, termination of your employment with Council. Council also retains the right to report any illegal violations to the appropriate authorities.

## **Responsibilities**

### **General Manager, Directors, Managers and Supervisors**

- Ensuring that staff have an understanding of the Internet, Email and Mobile Computing policy and procedures.
- Implementing disciplinary procedures when there has been improper use of the Internet and/or email.

### **IT Services**

- Ensuring that all authorised users who have Internet access have signed an Internet and Email Usage Agreement.
- That all computers used to access the Internet and email have approved anti-virus software installed and operational.
- Monitoring Internet and email usage across Council.
- Reporting misuse of these facilities to their Director.

### **Human Resources**

- Ensure the Employee's signed Internet and Email Usage Agreement is scanned and registered to the employee's personnel file.

### **Internet Coordinator**

- Administers and moderates Council owned External Distribution Email Lists and Social Networking Sites and Community facing web sites for all material and content published.
- Administers the authorisation of publication and moderation rights to authorised users where applicable to maintain Council owned External Distribution Email Lists, Social Networking Sites and Community facing web sites.

### **Staff, Contractors and other Authorised Users**

- Reporting to their Manager the receipt of unacceptable material from either external or internal sources.
- Ensuring that their use of Internet and email access is appropriate and consistent with ethical conduct under this policy and with regard to the Model Code of Conduct.
- Have read and ensure that they understand any correspondence from the IT Services section with regard to Virus Warnings. If any staff are in need of clarification of any correspondence they are to contact IT Services before further utilising any computer software or hardware.
- Ensuring that all General Principles and the Conditions of Use as detailed herein are adhered to at all times.
- Monitoring the use of their computer by others for Internet purposes and ensuring that other staff who use their computer are aware of this policy.

## Conditions of use

1. All Web browsing during business hours is to be for an organisational need and usage will be monitored to ensure that this is followed.
2. File download is permitted, with the exception of application and operating system files. The files are to be downloaded to the appropriate directory.
3. The use of and access to "streaming" Internet sites is not allowed except with prior approval of the Manager IT Services for each instance, and only in the cases where it directly relates to the business of Council. These sites may include, radio stations, media sites, music sites (video or audio), film/movie/mpg sites and sports relay sites.

### Users MUST:

4. Be respectful of all individuals and communities with which they interact via the Internet, Email and/or whilst using Social Networking Sites.
5. Be polite and respectful of others' opinions, even in times of heated discussion and debate over the Internet, Email and/or whilst using Social Networking Sites.
6. Adhere to these Conditions of Use, and seek to conform to the cultural and behavioural norms of any Social Networking Site being used over the Internet.

### Users shall NOT:

7. Breach any applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.
8. Use Council's Internet to visit Internet sites that contain obscene, hateful or other objectionable materials; send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
9. Use Council's Internet or email for the purpose of gambling.
10. Solicit emails that are unrelated to business activities.
11. Solicit non-Council business for personal gain or profit.
12. Use Council's Internet or email for any illegal purpose.
13. Use Council's Internet for accessing personal social media accounts.
14. Attempt to obscure the origin of any message or download material under an assumed Internet address.
15. Represent personal opinions as those of Mosman Council.
16. Make or post indecent remarks, proposals, or materials.
17. Upload, download, or otherwise transmit commercial or any other executable software or any copyrighted materials belonging to parties outside of Council, or to Council itself.
18. Download any software or electronic files without ensuring compliance with Council's approved virus protection measures and procedures and licences.
19. Intentionally interfere with the normal operation of the network, including by the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.
20. Reveal or publicise confidential or proprietary information which includes, but is not limited to:
  - financial information;
  - Council business, strategies, plans, databases and the information contained therein;

- client, ratepayer, resident or other community information;
  - technical information;
  - computer/network access codes; and
  - information about Council's business relationships which they are not authorised to release, reveal or publicise.
21. Examine, change or use another person's files, output or user name for which they do not have explicit authorisation.
  22. Perform any other inappropriate activities or uses on the computer network as may be identified by the Manager IT Services.
  23. Waste time on non-Council business.
  24. Remove, disable, modify or interfere with in any way Virus Software loaded on any Council computer unless under direct instruction by the IT Services section.
  25. Download large files such as MP3, Video, broadcasts, etc which are not work related.
  26. Attempt to circumvent Council's security controls or attempt to illegally access a computer (hacking).

## **Usage of email and/or the Internet on Mobile Devices**

### **Council Provided Mobile Equipment**

Usage of email and Internet over a Broadband service provided as part of the Authorised user's Mobile Phone, Mobile Tablet (iPad) or Laptop computer is subject to all the above principles, conditions of use and rules.

Authorised users must ensure that they use strong passwords, and regularly change these passwords, when accessing their mobile devices, to ensure the privacy and security of Council information held or accessed through these devices.

If a Mobile Device is lost or stolen, the Manager IT Services must be advised immediately to ensure that the Authorised Users passwords and access to the Council's computer systems are locked to prevent any possible breach of Council's Network.

Authorised users are directed to read the above terms in conjunction with Council's Mobile Phone Policy.

### **BYOD (Bring Your Own Devices)**

Use of a Personal / Private Mobile device with an authorised Council provided email account must be approved by the authorised users Director and the Manager IT Services, and is thereafter subject to all the above principles, conditions of use and rules as if it was a Council provided mobile device.

## **Usage of Social Networking Sites in a personal Capacity**

Notwithstanding the Guiding Principles and Conditions of Use of the policy detailed above, Council recognises social media and social networking sites are an increasingly common tool to engage in conversations with individuals and the community in a personal capacity.

Users who choose to make references to Mosman Council, its staff or services in a personal capacity must:



- ensure in these circumstances that readers of their post do not misconstrue personal comments as representing an official Council position.
- identify themselves as a Council employee;
- ensure they do not imply in any way that they are authorised to speak on Council's behalf;
- ensure they do not knowingly use the identity of another Council employee;
- be mindful during these engagements of the importance of not damaging the Council's reputation, commercial interests and/or bringing Council into disrepute;
- only disclose publicly available information. If they require clarification about what Council information is in the public domain, they should refer to material on the Council website ([www.mosman.nsw.gov.au](http://www.mosman.nsw.gov.au)) and or the Council annual report. They could also consult with the Manager Governance or Manager Finance;
- not include Council's logos or trademarks in their posts;
- be personally responsible for the content of their posts online;
- ensure any information about Council services provided is informed and factually accurate;
- use a disclaimer to ensure that their stated views and opinions are understood to be their own and not those of Council.

## Definitions

### Access

Access to the Internet and email will be limited to staff who have demonstrated to the satisfaction of their Director that access is required to support their day-to-day work.

### Adware

A form of Malware which propagates from unsolicited advertising on the computer.

### Authorised Users

Comprises Council Employees, Councillors, Council contractors and/or other persons assigned with access to Council's Computer Systems.

### Blog

Usually a personal journal published on the World Wide Web consisting of discrete entries ("posts") typically displayed in reverse chronological order. They are usually the work of a single individual, occasionally of a small group, and often are themed on a single subject.

### Chat room

Primarily used by mass media to describe any form of conferencing, to share information via text with a group of other users. The users in a particular chat room are generally connected via a shared interest or other similar connection. The term can apply to any technology ranging from real-time online chat over instant messaging and online forums to fully immersive graphical social environments.

### Email

A system that provides a convenient and effective means of communication between divisions, departments, branches, and individual staff in Council. Where installed, the additional capability of using the Internet for external email extends this convenience to any other group or organisation with an Internet mail address.

### Internet

An unregulated, worldwide network, linking thousands of computers and millions of people. It makes it possible to rapidly share information around the world.

### **Internet forum, or message board**

An online discussion site where people can hold conversations in the form of posted messages. They differ from chat rooms in that messages are at least temporarily archived. Also, depending on the access level of a user or the forum set-up, a posted message might need to be approved by a moderator before it becomes visible.

### **Intranet**

An internal system that allows the rapid share of information, usually limited to staff, but not necessarily limited to just staff.

### **Malware**

Consists of Spyware, Adware and other malicious code which can damage or appropriate data, or take control of computers.

### **Security**

The Internet and emails should be regarded as an inherently insecure environment. Confidential information should not be transmitted via these mediums. No personal information should be transmitted without the consent of the individuals concerned.

### **SPAM**

Also known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients usually intending to sell items and/or including chain-letters, hoaxes or other non-business related content.

### **Spyware**

A form of malware which typically tries to enter a computer attached to the internet via hidden code in a web page which is accessed. This code may then attempt to log keystrokes, corrupt and steal information and place control of the equipment in the hands of an outside party.

### **Social Networking Sites**

Websites, including but not limited to Facebook, Twitter, Flickr, and Myspace; that focus on building networks of personal relationships among people, who share like interests and/or activities. A social network site consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network sites provide means for users to interact over the Internet, such as e-mail and instant messaging.

### **Virus software**

Anti Virus software is an application that starts on all of Council's computers during initial startup. It is one of the tools used by Information Technology Services section in ensuring the integrity of Councils network and data. The term Virus Software is not limited to mean any specific application, but may from time to time include other brands and styles of protection as deemed necessary by the IT Services section.

### **World Wide Web (WWW)**

Is an application that runs on the Internet. It gives the ability to easily search interconnected computers and jump to any of those computers at the click of a mouse button. The application's most common interface is the graphical browser; the application selected by council for its WEB browser is Microsoft Explorer.

## **Authorisation**

This policy was authorised by the General Manager.

## **Document Owner**

The Manager IT Services is responsible for maintaining the accuracy and relevance of this policy.

## **References/Legislation**

Privacy and Personal Information Protection Act 1998

Privacy and Personal Information Protection Regulation 2005

Government Information (Public Access) Act 2009 No 52

Government Information (Public Access) Regulation 2009

State Records Act 1998 No 17

State Records Regulation 2010

Workplace Surveillance Act 2005 No 47

Workplace Surveillance Regulation 2005

Mosman Council Code of Conduct

\* Council acknowledges the work of Telstra and other Local and State Authorities used in the development of this policy.

## Internet, intranet & email usage agreement

I, (print name) \_\_\_\_\_ acknowledge that I am being granted Internet and email access using Council facilities in order to carry out my work and agree that my use of the Internet will be conducted in an ethical and professional manner.

I agree that I will not use this access for personal use during scheduled hours of work. I also agree that personal use will not include inappropriate behaviour such as access to or downloading from offensive sites; personal (non work related) postings to Internet forums such as Social Networking Sites, Newsgroups or Blogs; or activities for personal financial gain.

I understand that I have been given notice in accordance with section 10(2) of the Workplace Surveillance Act 2005 (NSW); and that Council will be entitled to, and shall commence monitoring, all my personal and business use of these services and communication facilities, and that monitoring will be in accordance with this policy and that inappropriate usage may be cause for disciplinary action up to (but not limited to) written warnings and revocation of access privileges.

I understand that my use of the Internet and email is identifiable by others as a Council activity and acknowledge that it is my responsibility to ensure that my usage does not contravene any laws or regulations, including copyright and licensing issues and laws respecting obscene and discriminatory material. I agree that I will not transmit sensitive material via the Internet or email or any forms of social media.

I understand that if I am not prepared to accept any of these conditions of this policy that access to email and internet facilities will NOT be granted.

I understand by signing this document I acknowledge that I have read and understood this document. I further understand that it is my responsibility to seek advice regarding any questions I might have regarding this document prior to my signing.

Signed \_\_\_\_\_  
Date \_\_\_\_\_

Witness Signature \_\_\_\_\_  
Witness Name \_\_\_\_\_