

POLICY:-	
Policy Title:	Internet and Email Policy
File reference:	F10/618-05
Date Policy was adopted by Council initially:	21 October 2004
Resolution Number:	267/04
Other Review Dates:	19 March 2009, 21 June 2012
Resolution Number:	117/09, 187/12
Current Policy adopted by Council:	20 September 2018
Resolution Number:	272/18
Next Policy Review Date:	2021

PROCEDURES/GUIDELINES:-	
Date procedure/guideline was developed:	N/A
Procedure/guideline reference number:	N/A

RESPONSIBILITY:-	
Draft Policy Developed by:	Director of Finance and Administration
Committee/s (if any) consulted in the development of this Policy:	N/A
Responsibility for implementation:	General Manager
Responsibility for review of Policy:	Director of Finance and Administration

OBJECTIVE

The objective of this policy is to identify the acceptable use of Council's Internet, email and mobile computing systems; i.e. laptops and Ipads.

POLICY STATEMENT

The Upper Lachlan Shire Council recognises that email is a modern method of communication that utilises the Internet and enhances the timely sharing of information, improves staff productivity and increases customer accessibility to Council. Council identifies that the adoption of email systems will promote communication between Council and its community.

Upper Lachlan Council provides email to its employees for the purposes of facilitating the work of Council and supporting associated communication processes. The email system is also provided for the public, and people who deal with Council, as an additional avenue of communication to Council. Additionally, email has been adopted as a tool to support Council in facilitating on line service delivery to its community.

The email system and its contents remain the property of Council. It is acknowledged that email messages constitute organisational records. Council reserves the right to manage, store, records manage, maintain and repair the email system and its contents, and investigate illegal use or wrong doing. Misuse of email and Internet systems will result in disciplinary action and / or litigation if necessary.

Internal email use is to be restricted to the staff and Councillors of Upper Lachlan Shire Council and authorised persons as delegated by the General Manager. Email and Internet services are provided to Council staff for work related use. During business hours Council staff are to limit their personal use of Council's email and internet systems so as not to interfere with the business function or processes of Council. However, personal use of these systems is allowed outside business hours, as long as it is in accordance with this policy and not of an excessive nature.

Internal and outbound email use should conform to current legislation, and support Council's Operational Plan, vision, mission and strategic direction. Protocols for email use have been developed to support this policy.

BACKGROUND

The Internet is a world-wide computer and communications network used by all sectors of the community for a variety of purposes.

The Internet is not a single network, but rather a collection of computer networks linked through well-defined interfaces. The lack of any central authority controlling or developing services presents certain drawbacks which staff should be aware of. Issues of concern, recognised within the Internet community, include:-

- | | |
|-------------------|---|
| Confidentiality - | The Internet should be regarded as an inherently insecure environment. Confidential information should not be transmitted on the Internet. |
| Data Protection - | Do not publish or distribute personal information without the consent of the individuals concerned. The transmission of personal data of third parties should be avoided. |

Copyright and Intellectual Property Rights must be observed.

Security Issues - The open nature of the Internet increases the risk of unauthorised access to networks and data. The maintenance of appropriate security measures is essential to ensure the confidentiality, integrity and availability of the Shire's data.

INTERNET GATEWAY MANAGEMENT

The Information Technology section of the Finance and Administration Department is responsible for the management of all Internet gateway services, including the maintenance of security and firewall facilities.

The Internet gateway must be used for all Wifi/LAN-based access to the Internet. No unauthorised access is allowed, this includes remote access via software such as TeamViewer, VNC, VPN software. All outgoing and incoming Internet traffic must be routed through the firewall and gateway facilities.

ADMINISTRATION OF INFORMATION SYSTEMS

The Information Technology (IT) section of the Council's Finance and Administration Department is responsible to ensure the efficient use of Internet and email systems in accordance with this Policy. Council will ensure that email documents are properly managed for record keeping purposes. Directors and Managers are responsible to ensure the continued understanding of the policy and its protocols by Council staff.

Users need to be aware that under normal operations, all Internet traffic and web browsing is logged. All email traffic is logged and archived. This information is used to determine any major load or performance issues, and that during this process individual information may be viewed by Information Technology staff. If required, individual reports of email and Internet usage and copies of individual emails can be produced from these log and archive files.

All users are to have individual passwords to log onto the Council network for security purposes. All users are to maintain confidentiality of their login password.

The Council appointed Administrator is the Information Systems Coordinator. The Information Systems Coordinator and the IT Systems Support Officer will have access rights to all user passwords. These designated IT Council Officers shall not disclose Council staff user passwords and will only use these details in their responsibility of administering corporate information systems.

INTERNET AND EMAIL USAGE

Council fosters an environment where all staff are assured that the privacy of their communications will be respected as long as they abide by the organisation's stated policies.

While Council's information systems do allow the logging and screening of network activity in certain circumstances, the Council does not support pervasive and systematic surveillance of staff emails and web logs.

All users are to be conscious of the fact that improper use of email and Internet may pose a threat to Council information systems security and the legal liability of the Council organisation.

Access Restriction - Web browsers will be configured to screen and restrict access to sites that fall within specified prohibited categories.

Software - Use of non-standard Internet software is prohibited. Modification of standard Internet software to bypass security measures is prohibited.

All users are to be aware that large files and email attachments can have a detrimental effect on Council's computer systems performance. Where a business need for cloud based transfer of information is identified, Dropbox is Council's preferred software for the transfer of corporate files to and from relevant contacts. If Employees require access to Dropbox, they must lodge a request to Information Services Staff who will confirm the business need and arrange approval from the relevant Department Manager.

CONDITIONS OF USAGE

- The Internet and email system may be accessible to all Council staff.
- Internet use is limited to reasonable use that supports the Upper Lachlan Shire Council's business.
- The Internet may be used for web browsing for work related activities.
- The Internet is not to be used for games or for excessive personal use.
- The use and access to 'streaming' Internet sites is not allowed. These sites may include radio stations, media sites, Skype, music, sport and movie sites.
- Council staff may not use and access social media or social networking sites for personal use during working hours; i.e. Facebook, Twitter, Instagram and MySpace.
- Internet etiquette is to be observed at all times.
- Council staff may use Internet services for personal development and/or professional development, outside Council working hours, provided it is not used for personal financial gain.
- Users should not open attachments from emails where they do not recognize the sender as they could potentially be malware. Any alert reported by the antivirus software or unusual computer activity should be reported to Information Systems staff immediately.
- For security reasons users who receive Council confidential or restricted information via email must not forward these Council email messages to their own personal third party web based email account unless authorised by the General Manager. In circumstances where it is necessary to transmit

confidential or restricted information via email the sender must ensure the following checks are carried out prior to sending the information:

- ◆ the name and address of the intended recipient(s) are correct; and
 - ◆ the email message is clearly marked as 'Private and Confidential'
- When employees go on leave, it is their responsibility to ensure an out of office reply has been set for their email prior to their leave commencing.

ABUSE OF USAGE

Any user who, in the opinion of the General Manager, is considered to have abused the Internet service and email facility will have their access to the service(s) removed and may lead to disciplinary procedures.

The accessing of websites that are not directly related to the completion of Council business, during working hours, is to be kept to a minimum. Personal emails, while available to all users during working hours, shall not interfere with the business operations of Council.

Council will revoke the use of Internet and email systems because of misuse or serious abuse of usage by Council staff as listed below:-

- The sending of unsolicited emails (i.e. SPAM, chain letters and junk mail).
- Conducting business other than Council business, (i.e. secondary employment) without the approval of the General Manager.
- Promotion of a personal or commercial benefit.
- Violation of a copyright.
- Sending of malware including viruses or other destructive content.
- Sending and/or disclosing of inappropriate content (i.e. illegal, immoral, offensive or obscene material, pornographic, erotic images, race or religious based material).
- Sending emails using offensive language.
- Sending, disclosing and/or distributing personal or confidential information held by Council.
- Sending, disclosing and/or distributing slanderous and/or defamatory material.
- Sending emails as a form of harassment, bullying or threatening behaviour.
- Any act that contravenes a law or is a criminal offence.
- Any act that may have a negative impact to Council.

CRIMINAL ACTIVITY

Hacking and illegal use of the Internet and any related criminal activities will result in the matter being referred to the Police for investigation and / or ICAC if necessary.

STAFF ACCESS TO THE INTERNET

Internet and email services are available to all staff. The downloading or receipt via email of executable or program files from LAN-based workstations is prohibited without permission from Council's General Manager.

VIRUS SCANNING

Council's Information Technology section shall ensure current virus scanning software is integrated with Internet services and will monitor executable and program files on the network.

The use of unauthorised software is strictly prohibited. Unauthorised software may be deleted from workstations and user areas on network drives without warning.

EMAIL ETIQUETTE

Email should not be regarded as a secure medium. Email messages transmitted over the Internet may pass through many computer systems as they are routed to their destination. Messages can be intercepted and scanned for keywords and interception is undetectable.

Private email can be used infrequently, providing it does not interfere with work. All personal outgoing emails must include the following standard disclaimer:-

This message is intended for the addressee named and may contain confidential information. If you are not the intended recipient, please delete it and notify the sender. Views expressed in this message are those of the individual sender, and are not necessarily the views of the Upper Lachlan Shire Council, unless otherwise stated.

Subscription to mailing lists, unless work related, by Council employees, is prohibited. Email traffic may be monitored by Council's Information Technology section.

Accessing, or attempting to access, the email messages of another employee is prohibited and shall invoke disciplinary procedures. Council will access email messages only at the instruction of the General Manager or Police if there is suspected illegal use or evidence of abuse by a Council user.

RESPONSIBILITIES

General Manager, Directors and Managers

1. Ensuring that Council staff are aware of and have an understanding of the Internet and Email Policy and received a copy of the same;
2. Ensuring that Council staff comply with the "Conditions of Usage" requirements of the Internet and Email Policy; and
3. Implementing disciplinary procedures, in accordance with Council's Code of Conduct and Disciplinary Policy, where there is proven misuse or improper use of Council's Internet and/or email systems by Council staff.

Information Systems (IT) Officers

1. Implementation and network administration of access for Council staff to Internet and email services; and
2. Reporting misuse (as per “Abuse of Usage” clause) of Council Internet and email services to the General Manager and relevant Departmental Director.

Council Staff, Councillors, Contractors and Authorised Users

1. Have read and understood the Council Internet and Email Policy;
2. Adhere to the “Conditions of Usage” requirements as detailed herein the Council Internet and Email Policy;
3. Ensure their use of the Internet and email is consistent with ethical behaviour under the Council Internet and Email Policy and Code of Conduct;
4. Ensure that Council’s Records Management Policy is adhered to and all relevant work related documents, such as emails, are registered into Content Manager document management system;
5. All staff are responsible to regularly review their email account, action emails, and reduce the size and content of their user account as this has the potential to impact on Council information systems; i.e. WAN speeds and available space on Council servers; and
6. Report to their Manager and Information Systems Coordinator the receipt of unacceptable material from internal or external sources to allow blocking.

LEGISLATIVE PROVISIONS

Reference should be made to the following legislation, guidelines and policy documents when reading this policy:-

Local Government Act 1993;
Local Government (General) Regulations 2005;
Independent Commission against Corruption Act 1988 and ICAC Guidelines;
Work Health and Safety Act 2011 and Regulations;
Anti Discrimination Act 1977;
Local Government (State) Award 2017;
Fair Work Act 2009;
Equal Employment Opportunity Act 1987;
Government Information (Public Access) Act 2009;
Privacy and Personal Information Protection Act 1998;
Environmental Planning and Assessment Act 1979;
NSW State Records Act 1998;
Industrial Relations / Workplace Surveillance Act 2005.
Code of Conduct for Councillors, staff and delegates of Council;
Council Information Technology Strategic Plan;
Council Records Management Policy;
Council Internal Control and Procedures Manual;
Council Bribes, Gifts and Benefits Policy;

Council Complaints Management Policy;
Council Government Information (Public Access) Policy;
Council Service Delivery Policy;
Council Fraud and Corruption Prevention Policy;
Council Public Access Policy;
Council Statement of Ethical Principles;
Council Social Media Policy;
Council Mobile Telephone Policy;
Council Disciplinary Policy; and
Council Information Services Guidelines (Appendix to this Policy).

REVIEW OF POLICY

Council reserves the right to review, vary or revoke this Policy.

APPENDIX

INFORMATION SERVICES GUIDELINES

One-to-One Communications

One-to-one communications are those in which a person is communicating with another person as if face-to-face: a dialogue. In general, rules of common courtesy for interaction with people should be in force for any situation and on the Internet it's doubly important where, for example, body language and tone of voice must be inferred.

User Guidelines

- Unless you are using an encryption device (hardware or software), you should assume that mail on the Internet is not secure. Never put in a mail message anything you would not put on a postcard.
- Respect the copyright on material that you reproduce.
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are reposting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.
- **Never send chain letters via electronic mail.** Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your system administrator if you ever receive one.
- A good rule of thumb: Be conservative in what you send and liberal in what you receive. You should not send heated messages even if you are provoked.
- In general, it's a good idea to at least check all your mail subjects before responding to a message. Sometimes a person who asks you for help (or clarification) will send another message which effectively says "Never Mind". Also make sure that any message you respond to was directed to you. You might be cc'd rather than the primary recipient.

- Make things easy for the recipient. Many mailers strip header information which includes your return address. In order to ensure that people know who you are, be sure to include a line or two at the end of your e-mail message with contact information. You can create this file ahead of time and add it to the end of your message.
- Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending.
- Watch cc's when replying. Do not continue to include people if the messages have become a 2-way conversation.
- Don't send unsolicited mail asking for information to people whose names you might have seen in documents or on mailing lists.
- Remember that people with whom you are communicating may be located across the globe. Allow time for the recipient to read mail, before assuming the mail didn't arrive or that they have not responded.
- Verify all addresses before initiating long or personal discourse.
- Know whom to contact for help. Usually you will have resources close at hand. Check locally for people who can help you with software and system problems. Also, know who to go to if you receive anything questionable or illegal. Most sites have a "Postmaster" aliased to a knowledgeable user, so you can send mail to this address.
- Remember that the recipient is a human being whose culture, language, and humour have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. Be especially careful with sarcasm.
- Use mixed case. **UPPER CASE LOOKS AS IF YOU'RE SHOUTING.**
- Use symbols for emphasis. That **is** what I mean. Use underscores for underlining. Be careful with slang and local acronyms.
- Be brief without being overly terse. When replying to a message, include enough original material to be understood but no more.
- Mail should have a subject heading which reflects the content of the message.
- If you include a signature keep it short. Rule of thumb is no longer than 4 lines. Remember that many people pay for connectivity by the minute, and the longer your message is, the more they pay.
- If you think the importance of a message justifies it, immediately reply briefly to an e-mail message to let the sender know you got it, even if you will send a longer reply later.
- Be aware of the size of a message you are sending. Including files such as postscript files or programs might make your message so large it cannot be delivered or at least consumes excessive resources.

- Do not send unsolicited information to people.

One-to-Many Communications Mailing Lists

Any time you engage in one-to-many communications, all rules for e-mail should apply. After all, communicating with many people via one e-mail message is quite analogous to communicating with one person with the exception of possibly offending a great many more people than in on-to-one communication. Therefore, it is important to know as much as you can about the audience of your message.

User Guidelines

General Guidelines for mailing lists

- Consider that a large audience will see your correspondence. Take care in what you write. Remember too, that mailing lists are frequently archived, and your words may be stored for a long period and many people may have access.
- Assume individuals speak for themselves, and what they say does not represent their organisation (unless stated explicitly).
- Remember that mail takes system resources. Pay attention to policies covering their uses.
- Messages and articles should be brief and to the point. Don't wander off the topic, don't ramble and don't send mail or post messages solely to point out other people's errors in typing or spelling.
- Subject lines should follow the conventions of the group.
- Forgeries and spoofing are not approved behaviour.
- Send of advertising material is prohibited.
- If you are sending a reply to a message or a posting be sure you summarise the original to give a context. This will make sure readers understand when they start to read your response. But, do not include the entire original.
- Be careful when you reply to messages. Frequently, replies are sent back to the address which originated the post - which in many cases is the address of the mailing list. You may accidentally send a personal response to a great many people, embarrassing all involved. It's best to type in the address instead of replying on "reply".
- If you find a personal message has been sent to a list or group, send an apology to the person and to the group.
- If you should find yourself in a disagreement with one person, make your responses to each other via e-mail, rather than continue to send messages to the list. If you are debating a point on which the group might have some interest, you may summarise for them later.

- You should avoid disagreements by email correspondence. Neither post nor respond to incendiary material.
- Posting articles or sending messages to a group whose point of view is offensive to you simply to tell them they are offensive is not acceptable. Sexually and racially harassing messages will have legal implications.
- Send subscribe and unsubscribe messages to the appropriate addresses. It is your responsibility to learn how the lists work, and to send correct mail to the correct place. Be sure you know the conventions for subscribing and unsubscribing.
- In general, it is not possible to retrieve messages once you have sent them. Even your system administrator will not be able to get a message back once you have sent it. This means you must make sure you really want the message to go as you have written it.
- If you ask a question, be sure to post a summary. When doing so, truly summarise rather than send an accumulation of the messages you receive.
- Some mailing lists are private. Do not send mail to these lists uninvited. Do not repost e-mail from these lists to a wider audience.

