GENERAL POLICY

Information Technology and Computers

2017

MAPOON ABORIGINAL SHIRE COUNCIL
30 Main St, Mapoon, QLD. 4874

PREFACE

Mapoon Aboriginal Shire Council is required by law to have a policy with clear guidelines and processes designed to protect the organisation from Risk and to effectively assign responsibility for users of the information tools and systems provided

In this section:

- Policy Statement
- Accountabilities
- Contact
- Related Information

POLICY STATEMENT

The intranet, Internet and electronic mail (email) are important business, teaching and learning tools that can enhance workflow, increase productivity and help Mapoon Aboriginal Shire Council (MASC) officers perform a variety of tasks; as such they should be used in an efficient, lawful and ethical manner.

MASC officers are accountable to the council for appropriate use of these technologies and should abide by the Intranet, Internet and Email Usage Policy.

Accountabilities

1. Intranet, Internet and email access is provided for officially approved purposes only i.e. council business and limited personal use (as defined in Procedures section of the Intranet, Internet and Email Usage Policy).
2. MASC officers must comply with all policies, legislation and regulations applicable to the use of the intranet, Internet and email.
3. Intranet, Internet and email usage should be able to withstand public scrutiny and/or disclosure. Unauthorised access, transmittal or storage of material that might bring the council into disrepute is prohibited.
4. Council information should not be transmitted or made available via the intranet, Internet or email except under council approved protocols.
5. MASC officers should not use the intranet, Internet or email in a way that could defame, harass, abuse or offend other intranet, Internet and email users, individuals or organisations.
6. MASC officers should not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, malicious or pornographic material.
7. MASC officers should not disrupt or interfere with the use of intranet, Internet or email services.
8. MASC officers should keep their user-ID and passwords secure. They should not reveal to others or allow others to use their user-ID or passwords.
9. MASC officers should not attempt any unauthorised access of intranet, Internet or email services. Unauthorised access includes, for example, the distribution of messages anonymously, use of other officers' User IDs or using a false identity.
10. MASC officers should not knowingly obtain unauthorised access to information and should not damage, delete, insert or otherwise alter such information carelessly or with malicious intent.
11. MASC reserves the right to monitor and audit any or all intranet, Internet or email activity undertaken by MASC officers using council resources. MASC officers may be called on to explain their use of the intranet, Internet or email.
12. Electronic messages and electronic files are subject to record keeping, archiving, freedom of information and legal process.
13. Violations of council policy may result in restriction of access to technologies, disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

Contact

For further information contact:

(a) CEO (copyright, freedom of information and legal process)
(b) Future Computers (technical issues)
(c) CSM (appropriate action for breach of policy including potential disciplinary action)

Related Information

Public Sector Ethics Act 1994 (Qld)
Queensland Government Use of the Internet and Electronic Mail Policy and Principles Statement
Anti-Discrimination Act 1991 (Qld)
Copyright Act 1968 (Cwlth)
Criminal Code Act 1899 (incorporating the Criminal Code
Defamation Act 1889 (Qld)
Freedom of Information Act 1992 (Qld)
Libraries and Archives Act 1988 (Qld)
Financial Management Standard 1997 (Qld)
Evidence Act 1974 (Qld)
Electronic Transactions Act (Cwlth) 1999
Broadcast Services Act 1992 (Cwlth) — Schedule 5
Privacy Act 1988 (Cwlth)
Classification (Publications, Films and Computer Games) Act 1995 (Cwlth)
Queensland Information Standard 38: Use of Communications and Information Devices

PROCEDURES

In this section:

---

1 Scope

1.1 This policy identifies the principles for the access to and proper use of council intranet and Internet services; capture of, access to, review and disclosure of email messages; and the proper use of email services provided by the council.

1.2 This policy applies to:

(a) All intranet, Internet and email services within Mapoon Aboriginal Shire Council (MASC), including those managed by external providers;
(b) All MASC officers who utilise, support or manage these services;
(c) All MASC officers who utilise council services for council business regardless of their location.

---

2. Objectives

2.1 The objectives of this policy are to:

(a) Protect MASC officers by informing them of the rights and responsibilities associated with use of intranet, Internet and email services;
(b) Prevent misuse of council assets;
(c) Protect the council from legal liability;
(d) Protect intranet, Internet and email services from attacks and outages;
(e) Protect against loss of information;
(f) Ensure capture and retention of corporate electronic records.

2.2 This policy cannot be totally exhaustive. Where situations not covered by this policy arise, contact your supervisor or refer to the contact information provided in the Preface.

---

3 Usage of this document

3.1 All MASC officers who utilise, support or manage intranet, Internet or email services should be aware of this policy, which includes their responsibilities and legal obligations.

4 Compliance

4.1 All MASC officers are required to comply with council policy and are bound by law to observe applicable statutory legislation relating to personal data, company data, public records, copyright and other forms of intellectual property and misuse of information and facilities.

5 Definitions

5.1 Corporate Records: Corporate records are information recorded in any form, including data in computer systems and data created, received and maintained by MASC officers and systems in the transaction of business or the conduct of affairs and kept as evidence of such activity. MASC corporate records are deemed as public records within the meaning of the Libraries and Archives Act.

5.2 MASC Officers: The term 'MASC officers' or 'officers' refers to all MASC permanent, temporary, seconded or contracted staff and consultants. Volunteers who assist staff with their professional duties and utilise council intranet, Internet and email services are also classified as MASC officers for the purposes of this policy.

5.3 Email messages: An electronic mail (email) message is a computer-based message sent via the communication network to one or more recipients. An email message may be transmitted with one or more attachments i.e. files containing text, graphics, images, digitised voice, digitised video or computer programs.

5.4 Integrity: Sound, undiminished and unimpaired condition.

5.5 Internet: The Internet is a worldwide loose affiliation of interconnected computer systems, through which users can navigate to obtain services and share information with globally dispersed organisations and individuals. Internet services include, but are not limited to chat, newsgroups, websites, games, banking, share trading, FTP (File Transfer Protocol) and Telnet.

5.6 Internet Mail: Internet mail is an email facility that enables users to send and receive messages to and from anyone that subscribes to the Internet mail service.

5.7 Intranet: The intranet is essentially a private Internet operating on MASC's internal network, protected from Internet users by a firewall. The intranet can be viewed as an information utility for MASC.

5.8 World Wide Web (WWW or Web): The web is an application on the Internet using a technology called 'hypertext' to create and link information. Web pages within a site typically have links within them, so that a user can click on an underlined word, a picture or a sound bite and be 'transported to' or 'pointed towards' another location within the same document or to another website. Web pages use Hypertext Mark-up Language (HTML) to create these links and pages can be viewed by any HTML capable client software or browser.

6. MASC Officers' responsibility

Summary

6.1 All MASC officers are expected to take reasonable precautions to protect intranet, Internet and email information and systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.

6.2 Specifically this includes:

(a) Understanding and complying with the security rules of these services;
(b) Using available mechanisms and procedures to protect their own information, information under their control and information downloaded from the intranet or Internet;
(c) Not providing or allowing inappropriate access to information, and not discussing it with others;
(d) Being accountable for authorising or allowing access to information they create on behalf of the council;
(e) Obtaining appropriate authorisation in order to access restricted information;
(f) Not attempting any unauthorised access to information and systems, whether internal or external, including email services and intranet and Internet services or sites;
(g) Using anti-virus software (standard anti-virus software where available) as identified in this policy;
(h) Maintaining security and confidentiality of user-ID and passwords;
(i) Reporting to their supervisor any suspected unauthorised access by others to the network using their user-ID and password;
(j) Reporting to their supervisor any inappropriate use of intranet, Internet or email services, or any suspected violation of this policy;
(k) Reporting to their supervisor any accidental access to inappropriate Internet sites;
(l) Ensuring corporate electronic records of continuing value are not destroyed prior to their capture on the appropriate official council record-keeping system.

Acceptable Use

6.3 The intranet service can only be used for council business purposes.

6.4 Internet and email services can only be used for:

(a) Council business
(b) Limited personal use

6.5 Council business use includes any activity that is conducted for purposes of accomplishing official business, professional duties including research and, where appropriate, professional development.

6.6 Limited personal use means use that is infrequent and brief. This use should generally occur during personal time and should not include uses:

(a) That require substantial expenditure of time;
(b) For private business, personal gain or profit;
(c) That impede the efficiency of intranet, Internet or email services;
(d) That clog mailboxes with large numbers of messages;
(e) That would violate or breach any State or Federal legislation and regulation;
(f) That would violate or breach the council Code of Conduct.

6.7 As a guide, use that occurs more than a few times per day and/or for periods longer than a few minutes would not be considered limited personal use.

6.8 Individual officers may be held personally responsible for any use of intranet, Internet and email services that does not comply with these principles.

Inappropriate Use

6.9 Inappropriate use of the intranet, Internet and email includes but is not limited to the points below.

6.10 MASC officers should not use intranet, Internet and/or email services to:

(a) Infringe the copyright or other intellectual property right of the council or third parties, for example, officers should not download and use work without the express permission of the owner. For further information refer to paragraph 7.1-7.3 — Copyright;

(b) Download software, unless they receive appropriate authorisation and comply with licensing requirements and established policies to check all such software for computer viruses;
(c) Scan and email print resources protected by copyright;
(d) Disrupt communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on council resources;
(e) Access inappropriate Internet sites;
(f) Download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet Sites;
(g) Download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity or religious and political beliefs;
(h) Download unreasonable amounts of material for non-council business use;
(i) Download information for the purpose of providing it to external organisations or the general public without authorisation;
(j) Distribute chain letters;
(k) Distribute defamatory, obscene, offensive, or harassing messages;
(l) Distribute confidential information without authority;
(m) Distribute messages that disclose personal information without authorisation;
(n) Distribute private information about other people;
(o) Distribute messages anonymously, using a false identity or using another person's email account;
(p) Engage in any illegal or wrongful activity;
(q) Engage in private business or personal profit ventures.

6.11 MASC officers may not:

(a) Disrupt or interfere with the use of intranet, Internet or email services;
(b) Without authority destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of intranet, Internet or email services;
(c) Misuse council resources, including human and computing resources.

Access to the intranet and Internet

6.12 Most MASC officers have access to the council intranet and selected Queensland Government Internet sites. Full access to Internet services is provided to MASC officers where it is appropriate to their professional duties; this access is considered on a case-by-case basis.

6.13 Officers should submit such requests to the CEO for consideration.

Inappropriate Internet sites

6.14 Inappropriate sites include but are not limited to:

(a) Sites that are illegal
(b) Sites that are pornographic or contain inappropriate adult sexual material
(c) Sites that advocate hate/violence
(d) Sites that offer inappropriate games or software

6.15 The downloading of information from inappropriate sites and the supply to others of inappropriate site addresses is prohibited.

Computer Systems Resource — A Finite Resource

6.16 MASC officers are reminded that computing resources are finite and are under increasing demand.

6.17 The Internet service is capable of placing a substantial burden on the council's computing resources. Therefore officers are expected to use the Internet service responsibly and with due regard to other users. For example, the download of large amounts of non-urgent information should occur during non-peak periods.

Listserv

6.18 A Listserv is a mailing list of peoples' names and addresses which is used to send messages or announcements to subscribers.

6.19 MASC officers can subscribe to Listservs that relate to the performance of their official duties. Officers are not permitted to subscribe to Listservs for personal interest or for purposes not related to official duties.

6.20 The rules and guidelines for the use of email also apply to the use of Listservs. For further information on Listservs refer to the IT manager.

Services for which a Subscription Fee is charged

6.21 There are many services available through the Internet on a user-pays basis. Where an MASC officer identifies a service which is relevant to their official work duties, an application to subscribe to the service should be made through the relevant manager. The MASC officer is responsible for checking whether there is a pre-existing subscription or some other means of accessing the information.

6.22 Under no circumstances should an officer enter into any subscription contract or agreement without the prior approval from the relevant manager.

Confidentiality

6.23 All MASC officers are expected to respect and safeguard all aspects of information confidentiality. Officers are expected to treat all council information, whether paper-based or electronic, as confidential. No one is permitted to disseminate council information outside the council without specific authorisation from the author or management. Officers should consider the author's intended use when disseminating information outside their work group/s.

6.24 Refer to the council's policy & procedures manual for more information on confidentiality and disclosure of official information.

Integrity

6.25 It is the responsibility of MASC officers to ensure access to the council network is kept secure. For example, if another officer uses your email account to send a message you are responsible for that message. Officers can achieve security by:

(a) Logging off the network or initiating a password-protected screen saver when they are out of the office or away from their desk;
(b) Ensuring their network and screen saver passwords are kept secure;
(c) Not revealing to others or allowing others to use their user-ID or passwords.

6.26 Refer to IT manager for additional information on integrity and security.

User-ID and Password Security

6.27 A common means of gaining illegal access to electronic information is to break a legitimate user's password. MASC officers should only select passwords that are not easy to guess or to find using a password-breaking program. Use the following guidelines to select and safeguard passwords:

(a) Keep passwords confidential.
(b) Do not write passwords down.
(c) Change passwords if compromised.
(d) When constructing a password use seven or more characters, and choose these characters from at least two of the categories of letters, cases, numbers and symbols.
(e) Avoid use of words which can be found in the dictionary.

(f) Avoid use of birthdays, pay or employee numbers, position numbers, addresses, family member or pet names or any other identification code that might be easily guessed or found in other information about the work unit or the account holder.

6.28 MASC officers who suspect access to the network has been obtained using their user-ID should immediately request a change of their password and notify their supervisor.

Use of Disclaimers

6.29 The following disclaimer should be included at the end of the signature block of email messages sent outside the council:

This message (including attachments) is intended for the addressee named above. It may also be confidential, privileged and/or subject to copyright. If you wish to forward this message to others, you must first obtain the permission of the author.

If you are not the addressee named above, you must not disseminate, copy, communicate or otherwise use or take any action in reliance on this message. You understand that any privilege or confidentiality attached to this message is not waived, lost or destroyed because you have received this message in error.

If you have received this message in error please notify the sender and delete from any computer.

Unless explicitly attributed, the opinions expressed in this message do not necessarily represent the official position or opinions of the Mapoon Aboriginal Shire Council.

Whilst all care has been taken, the Mapoon Aboriginal Shire Council disclaims all liability for loss or damage to person or property arising from this message being infected by computer virus or other contamination.

Capturing and Accessing email records

6.30 Email messages created, received or stored by officers in the conduct of or in connection with council business are deemed to be public records or documents within the meaning of the Libraries and Archives Act, Freedom of Information Act and Local Government Act 2009.

Requirements for retaining and enabling access to email messages include legislative imperatives such as the Libraries and Archives Act, Freedom of Information Act and legal process.

Libraries and Archives Act

6.30.1 Under the Libraries and Archives Act the council is required to make and keep complete and accurate records. Corporate council records created or received as email messages should be captured and stored in an accessible format for as long as they are required.

Freedom of Information Act

6.30.2 Any email messages, whether personal or business-related, may be accessed as 'documents' under the Freedom of Information Act and may, therefore, be subject to external scrutiny. This should be kept in mind when using email, particularly when conversing about confidential or politically sensitive subjects. Officers should also refrain from making comments about personalities or expressing personal opinions that may be considered derogatory or defamatory.

Legal Process

6.30.3 Emails (whether personal or business related) may be tendered in court as evidence and are subject to legal processes such as disclosure and subpoena.

Refer to section 95 of the Evidence Act and the Uniform Civil Procedure Rules for Supreme Court, District Courts and Magistrates Courts.

Storing and Deleting email messages

6.31 Appropriate record keeping of email messages is required under the Libraries and Archives Act.

Email messages can be deleted:

(a) If considered to be transitory messages of minor importance, once their administrative value ceases;

(b) If considered to be of continuing value, once a copy has been captured in the relevant official record-keeping system.

Any email message which is deemed to be a public record and which also has continuing value is currently required to be printed to hard copy and filed using the appropriate record-keeping system.

Messages of continuing value are those records that need to be kept for any length of time, varying from a few months to many years; and those which are required for use by others, affect the work of others or are required to be held for evidential, accountability or legal reasons.

Privacy of personal information

6.32 Personal information is confidential and can only be disseminated by authorised persons in specific circumstances. All officers are expected to respect and safeguard all aspects of information confidentiality.

Where personal information is being distributed with authority, the security of this information should be considered; refer to paragraph 8.1-8.4 — Security.

Privacy of email messages

6.33 Officers are not guaranteed privacy in relation to email messages, whether they are business-related or personal. The reasons for this include the following:

(a) Email is not secure, unless it has been encoded or encrypted.
(b) Email messages are hard to destroy. Email messages are backed up on a regular basis and can be recovered from these back-ups. The deletion of an email message from the email account does not remove the backed-up copy.
(c) Email messages are logged. These logs include email sender and recipient addresses, time of transmission and the content of the email. These logs are necessary for routine maintenance and management of the email service.

6.34 The council respects the right of officers to privacy, but the council reserves the right to:

(a) Access MASC officers' email messages, as defined in paragraph 6.35
(b) Monitor, access, examine and pass on messages, as per paragraphs 9.1-9.3 —Inspection and Monitoring

Officers are, however, granted reasonable licence to examine incorrectly addressed mail, but may not disclose it unduly.

Accessing email messages created by Officers

6.35 The council may seek to gain access to an officer's email messages, in the same way as for paper-based material, where this is necessary for the purpose of retrieving business information or for system maintenance.

In the case of system maintenance, the extent of access will not exceed the minimum essential for the performance of the maintenance function.

In the case of access to retrieve business information, the authority of the relevant manager is required before access is attempted, and the extent of access is restricted to no more than is necessary to locate and retrieve the relevant information.

Because it is a part of their official duties, Information Management officers have ongoing management authority to access and retrieve records created by other MASC officers.

---

7. Copyright

Copyright — Internet

7.1 Copyright laws protect most documents and software available through the Internet. MASC officers should consider the copyright implications associated with copying or otherwise reproducing Internet material. It is prohibited to use the Internet service to copy, reproduce or transmit any document, software (including HTML source code) or other information protected by copyright laws.

7.2 Officers should refer to the IT manager for further information on digital copyright

Copyright email

7.3 Use of the email system to copy and/or transmit any documents, software or other information protected by the copyright laws is prohibited.

---

8 Security

8.1 Email is a business tool that provides MASC officers with a means of internal and external communication. Not all of these communications are transmitted over a secure network; security is not assured where they are sent via Internet mail.

8.2 All messages sent outside the council organisation are sent via Internet mail.

8.3 All messages sent within and between council's offices are sent via the local area network and are therefore considered secure.

8.4 Email messages sent via Internet mail are easy to intercept and scan for key words of interest; this can be done routinely and automatically. Consider other means of distributing confidential or politically sensitive material.

---

9. Monitoring and Inspection

9.1 MASC reserves the right to monitor any or all Internet- or intranet-related activity and to monitor and inspect any or all email messages sent or received by MASC officers using council resources, in order to:

(a) Identify inappropriate use;
(b) Protect system security;
(c) Maintain system performance;
(d) Protect the rights and property of the council;

(e) Determine compliance with council policy;
(a) (c) Determine compliance with State and Federal legislation and regulation.

9.2 These monitoring and inspection activities include but are not limited to the following:

(a) Access and examination of specific types of messages e.g. large messages or messages containing executables, audio visual files, movie files, command files and/or pictures, in order to identify inappropriate use or to maintain system performance;
(b) Access and examination of messages in specific circumstances, such as where an individual's message volume is high or at the peak periods of Christmas and Easter or on a random sampling basis, in order to identify inappropriate use or to maintain system performance;
(c) Access, examination and referral of email messages for the purpose of complying with investigation requests received from Human Resources, Internal Audit, External Audit, Criminal Justice Commission, Freedom of Information, Senior Management or other authorities;
(d) Access, examination and referral of email messages for good cause or to satisfy legal obligations, in compliance with legislative requirements and council policies. Good cause includes the need to protect system security, identify inappropriate use and protect the rights and property of the council;
(e) Introduction and use of content security software to protect MASC officers and the council's computer network, systems and services from such things as viruses, offensive or libellous material and breaches of confidentiality.

9.3 Monitoring and inspection can apply to personal and business use of intranet or Internet services and personal and business-related email messages.

---

10. Consequences of Policy Violations

10.1 MASC officers' use of intranet, Internet and email services should be compliant with the principles and expectations laid out in this policy and the council's Policy & Procedures Manual.

10.2 Violations of this policy may result in restriction of access to intranet, Internet and/or email services and may lead to disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

10.3 Staff who are aware of or observe a suspected violation of this policy are responsible for reporting the incident to their supervisor.

---

11. Ongoing Development

11.1 It is intended that this policy continues to develop so that it keeps pace with council requirements and the progress of information technology. Requirements, suggestions and comments about these documents should be forwarded to the controlling officer identified in paragraph 12.1-12.3 — Responsibility.

---

12. Responsibility

Control and administration

12.1 The Information CEO (or delegate) is responsible for the control and administration of this policy.

Compliance

12.2 All MASC officers are responsible for ensuring that this Intranet, Internet and Email Usage Policy is observed.

Awareness

12.3 Workplace managers are responsible for ensuring that all MASC officers associated with their area are made aware of this policy.

---

13 Employee Acknowledgement

I, _____ hereby acknowledge that I have read the Information Technology and Computers policy and understand the terms as contained.

I agree, to the best of my ability, to do my best to support the policy terms and understand the roles and responsibilities as contained within.

_____	/	/	_____	/	/
Signature	**Date**		**Witness**	**Date**	

Schedule

In this section:

1. Electronic mail etiquette

1.1 The use of appropriate etiquette in email correspondence will make email a more effective communication tool and will be appreciated by recipients.

Think before you write

1.2 Before you create and send an email message, consider the following:

a) Is email the best medium for your message? Email is impersonal; without facial expressions and body language to provide clues, email can be misunderstood.
b) Are you overusing email? Don't let email replace all personal contact.
c) Consider the recipient's needs, if they do not need the information you will be saving them time by not sending the message.
d) Is this a council 'business transaction' which is likely to make this email and any subsequent emails corporate records? If so, how do I ensure their capture into the corporate record-keeping system?
e) Is email a suitable form of communication i.e. if highly confidential should the message be sent by email?

Style points

1.3 Consider the following style points:

(a) Maintain professionalism.
(b) Be succinct. The most effective email messages are short and to the point, but not so short as to be rude.
(c) Don't 'shout' by using upper case to emphasise a point you feel strongly about. This can set a negative tone.
(d) Keep the message focused on a single topic. Too many topics can cause confusion.
(e) Make it obvious what the email is about. State early on why the information is being sent, what is expected of the recipient/s and when the sender would like action, if any, to be taken.
(f) Appearance matters. Don't be sloppy or careless. Depending on the context, use of all lower-case letters or omitting punctuation may be interpreted as laziness or lack of respect for your reader/s.
(g) Consider message format. There is no guarantee that the user's email facility will display the message as intended. Do not depend on alignments, fonts and colours to make a point.
(h) Be courteous; don't forget please and thank you.

Good Sender Habits

1.4 Consider these good sender habits:

(a) Enter a meaningful subject that captures the content of the message. Replace vague subject lines with meaningful information, this helps recipients prioritise, file and search for messages.
(b) Use distribution lists with caution. Send email messages only to recipients who need the information.
(c) Tag messages appropriately. Do not tag messages as 'High Priority' or 'Urgent' if they are not.
(d) Do not 'reply to all' unless they all need to see your reply.
(e) Do not modify someone else's message.
(f) Address email according to the expected action. A person listed in the 'To' field is expected to respond; one in the 'CC' field is expected to read the message as information only.
(g) Before you forward messages to others consider the need to obtain the permission of the author. For example, consider the questions: Is the forwarding of the message compliant with the author's intended use of the information? Are you forwarding the message within your own work group?
(h) Choose the number and size of file attachments with care and avoid trivial attachments.
(i) Use graphics or pictures judiciously. Graphics or pictures as inserts do attract attention but use them sparingly as they add to the size of the email message, the time it will take to deliver the message and the load on the network.
(j) Review before sending. Proofread your correspondence and use the spellchecker; too many mistakes can make you look careless and can damage your professional reputation.
(k) Do not create or forward unsolicited email e.g. chain letters.
(l) If the email is a corporate record, print out a hard copy and file using the appropriate record-keeping system.

Good Recipient Habits

1.5 Consider these good recipient habits:

(a) Check your email at regular intervals.
(b) Use auto-replies or delegate authority when unable to check email.
(c) Browse the subject line or preview panel to identify important messages.
(d) File important messages into organised folders.
(e) Use inbox rules and filters to file messages automatically to relevant folders.
(f) Think before you reply. Many communications need no reply at all. Don't reply unless you have something significant and well considered to communicate.
(g) Reply or acknowledge receipt of messages promptly if the sender is expecting a response.
(h) Ask to be removed from unwanted distribution lists.
(i) Virus-scan attachments on emails received from external sources.
(j) Emails sent to external recipients should have the standard disclaimer at the end of the signature block.
(k) Delete junk mail.
(l) Print out and/or file corporate records and other important messages. The appropriate repository for filing will depend on your location and the task or subject to which this message relates.
(m) Delete messages that are no longer needed.

2. Effective Use of email

2.1 Email enables MASC officers to send messages to others both inside and outside the council. It is important for all officers to consider the implications of sending email messages to people who do not need them. The practice clogs mailboxes with unnecessary messages and wastes resources; ultimately it ends up impeding the communication system instead of enhancing it.

3. Use of attachments

3.1 Use attachments sparingly. Unnecessary use of attachments is a waste of space. Before you attach documents to an email message consider providing the recipient with either:

(a) Extracts of the relevant sections of the document rather than the whole document;
(b) A printed copy of the document or appropriate sections;
(c) The location of the document on the network.

4. Use of To, CC and BCC

4.1 Officers are advised to limit the number of recipients for an email message. Sending a message to a very large number of recipients can congest the network; if it is necessary consider sending separate messages to smaller groups.

4.2 The email service makes it possible to send information to more people faster than traditional communication methods. Just because it is faster does not mean it should be done; officers need to consider who actually needs to receive their message. Sending messages to recipients who do not need them is a waste of their time and system resources. As a guide, consider whether you would make a telephone call to all potential recipients of this message.

4.3 Officers need to be aware that under the Freedom of Information Act they are responsible for providing access, upon request, to every email message they send, receive and keep. Every person that an officer has sent or forwarded email to (via the 'To', 'CC' or 'BCC') is then required to be contacted by the investigating Freedom of Information officer.

4.4 Officers need to consider the intellectual property rights of authors before they forward messages to others. It is acceptable to send or forward council information to others within the council where it is relevant to their professional duties. Permission should be obtained from the author before sending or forwarding:

(a) Messages (including attachments) received from external sources;
(b) Messages (including attachments) outside the council.

5. Use of distribution lists

5.1 When an officer has a recurring need to communicate with a defined group of other officers, that officer can set up a distribution list identifying all the members of the group. Thereafter, the officer need only address messages to the group via the use of the distribution list; the email system sends the message to each member.

5.2 Exercise care when using distribution lists as they can become outdated. Use of out-dated distribution lists can waste time and resources.

6. Use of Broadcast emails

6.1 The email service should only be used for urgent broadcast messages, for example system shutdown alerts. Broadcast messages inappropriately sent via the email service can clog mailboxes and impede the efficiency of the service. Any officer wishing to send an email in this way must first log the request with the Information Management Help Desk for authorisation and dissemination.

7. Signature Block

7.1 MASC officers are encouraged to attach a signature block, containing the following minimum details, to every email message sent outside the council:

(a) Name
(b) Position

(c) Work Unit
(d) Full name of the council
(e) Email address
(f) Work phone and fax
(g) The signature block for email messages sent within the council is at the officer's discretion.

8. Inappropriate Internet Sites

8.1 Occasionally, officers can accidentally access inappropriate websites. Officers who do so should note the date and time, leave the site and notify their supervisor, in case monitoring highlights the access and a query is raised. Supervisors can forward the inappropriate site details to their relevant technical support area to have the site blocked.

8.2 Repeated access to unlawful sites will be referred to the appropriate authority **-** laws are in place to these carry serious consequence.

9. Spam Mail and Malware

9.1 Spam mail is basically electronic junk mail and MASC officers are receiving it in increasing quantities.

In general, senders of spam mail have two purposes:

(a) To encourage recipients to purchase goods or services from the sender;
(b) To gather live email addresses for future use or for on-selling.

9.2 Officers are requested not to respond to spam mail, even when the message provides an email address for you to request your email address to be removed from their lists. By responding you are confirming that the email address is live and the result will be an increase in the amount of spam mail received.

9.3 In some cases spam mail requests that the recipient visit a website, which may be a commercial site but could equally be an inappropriate site. In either case, the site will most likely have technology in place to gather identifying information about those who visit the site. It will almost invariably request that you provide personal details about yourself.

9.4 Spam mail increases transmission costs and takes up space in email accounts. Therefore, nothing should be done to encourage receipt of this type of mail.

9.5 If you are receiving large volumes of spam mail or spam mail that offers goods or services that are illegal, contact the IT manager for assistance.

9.5 Malware is malicious hardware which has been issued to purposefully infect your machine. This has malicious intent and is designed to infect and destroy.

9.6 Queensland Government - Office of Information Security will issue notices to government agencies and service providers regarding the latest information. This information must be issued to all staff and notice heeded.

10. Chain Letters

10.1 A chain letter is a communication which includes an incentive to forward it on to others. This incentive takes the form of a promise for reward and/or a threat.

10.2 Forwarding of chain letters is defined as an improper communication and therefore an inappropriate use of email services. Forwarding or sending of improper communications is a waste of council resources and may expose the council to risk of legal action or adverse publicity.

10.3 Improper communications are in breach of the Policy & Procedures Manual, and may be in breach of the law. As such they are prohibited by the council. **10.4** All chain letters should be deleted. If you are receiving large numbers of chain letters, contact your IT manager for assistance.

11. Defamation and Harassment

11.1 Distribution of defamatory or harassing messages is an inappropriate and improper use of email services. All MASC Officers should take care constructing the content of email messages to avoid potential claims of defamation, harassment or discrimination.

11.2 Harassment can take a number of forms including that based on gender, ethnicity, and religious and political beliefs. Harassing messages may leave the sender and/or the council liable under anti-discrimination laws and could lead to disciplinary action against the sender.

11.3 A statement is defamatory when its effect may be to destroy the personal or business reputation of another. Material can defame through use of words, pictures, a combination of these, or by innuendo. In some circumstances, defamation is a criminal offence.

11.4 Officers should also be aware of the effect that messages have on the reputation of the council. As a rule of thumb, when previewing email messages, officers should read the contents of the message as though they were liable to be publicly broadcast.

11.5 If you have received or have inadvertently sent a message that is or could be considered to be defamatory or harassing, contact your supervisor for assistance.

12. Document and Record Management Requirements

12.1 Every MASC officer is responsible for ensuring electronic records/documents of continuing value are placed in the appropriate record-keeping system for future retrieval.

12.2 It is the responsibility of authors of internal email messages and recipients of external email messages to determine whether the message is of continuing value and to take appropriate action. The following lists will assist you in determining whether a message is of continuing value, but this list is not exhaustive.

12.3 Examples of documents of continuing value include:

(a) Any document that relates to the conduct of council business;
(b) Approvals to undertake actions relating to council business;
(c) Formal communications between officers within the council, with other departments, with external organisations and members of the public;
(d) Formal minutes of meetings and committees;
(e) Final versions of reports;
(f) Amended versions of reports where instructions have been given;
(g) Policy documents;
(h) Advice given which may influence another person's actions in relation to council business.

12.4 Documents not considered to be of continuing value include:

(a) Personal messages not related to council business;
(b) Documents that do not relate directly to council business;
(c) Duplicated material e.g. an information-only copy of a document;
(d) Information distributed to a number of people e.g. circulars, meeting agendas;
(e) Drafts of reports or correspondence;
(f) Transitory messages of minor importance (e.g. telephone messages) which do not relate to council business;
(g) Messages which perform a similar function to an informal telephone call;

(h) Unsolicited messages seeking employment or offering goods or services to MASC.

12.5 Electronic messages may be deleted if considered to be records of continuing value once a copy has been forwarded to the relevant official record-keeping system. Electronic messages may be deleted if considered to be transitory messages of minor importance once their administrative value ceases.

Manager Responsible for Review:	**CEO**
Originally Adopted:	**05/2012**
Currently Adopted:	20/06/17
Due for Revision:	**30/06/2020**