Electronic Communications Policy

Strategic Reference	Objective 1; a caring, healthy and resilient community. Strategy 1.7; achieve or implement the statutory and core responsibilities of Council.
File reference	AR18/8676
Responsibility	Community & Corporate Department
Revision Number	4
Effective date	17 April 2012
Last revised date	May 2018
Minutes reference	086/18, 069/16, 031/14, 097/12
Next review date	Every two years, May 2020
Applicable Legislation	Local Government Act 1999
Related Policies	Elected Members' Code of Conduct Policy Code of Conduct Policy for Council Employees Information Security Policy Work Health Safety Policy Privacy Policy Records Management Policy
Related Documents	Electronic Communications Procedure

1. Purpose and scope

Coorong District Council recognises the need to embrace new and emerging technologies in conducting its business and fulfilling its objectives. Electronic communications utilising these technologies opens up opportunities for sharing information and the conduct of business. However it also brings with it an obligation to manage the risks associated with the use of these technologies in a coordinated way so as to build a legacy of dependable precedence and encourage consistency.

This Policy is fundamental to sound risk management. Regulating the use of electronic communications including Internet, email, social media and telephones is necessary to provide all Employees with a safe working environment and protect Council from commercial harm. Consequently all material sent, received, forwarded or transmitted may from time to time be subject to monitoring or retrieval by or at the direction of management.

Users should be aware that although there are access passwords and internal security systems there is general "insecurity" for communications exchanged via the Internet and email.

This policy applies to all users of Council technology, equipment and services. All persons who use or access electronic information, communicate electronically or otherwise use Council technology, equipment or services are bound by the conditions of this Policy. All rules that apply to use and access throughout this policy apply equally to equipment and facilities owned or operated by the Council wherever the equipment or facilities are located.

2. Definitions

"Electronic Communication" - includes but is not limited to:

- World Wide Web pages
- Electronic journals and texts
- Library catalogues
- Email
- Discussion lists
- Use Net news
- Internet relay chat
- Data of all kinds
- Social media
- Telephone systems, both mobile and land line
- Extranet
- Intranet
- Text messaging

"Email" – Is a service that enables people to exchange documents or messages in electronic form. It is a system in which people can send and receive messages through their computers or mobile telephones. Each person has a designated mailbox that stores messages sent by other users. Messages may be retrieved, read and forwarded or re-transmitted from the mailbox.

An ***"Employee"*** is any person who is employed by the Council, but also includes any contractors, volunteers, trainees, work experience students and consultants undertaking work for, or on behalf of the Council whether they are working in a full-time, part-time or casual capacity.

"Extranet" – a website specifically dedicated to information sharing between the Elected Members and the Leadership Team.

"Internet" – A global research, information and communication network providing services such as file transfer and electronic mail.

"Material" – Includes data, information, text, graphics, animations, speech, videos and music or other sounds, accessible electronically – including any combination or selection of any of these.

"Signature" – Is a signoff clause which allows you to add your own name, title, Council contact details, personal email address and direct telephone number etc at the end of outgoing mails.

"Hack" – To gain access into another's computer system or files by illegal or unauthorised means.

"Security System" – To protect the information on our networks we have prescribed controls giving authorisation and access to files and directories in the networks. Each individual has a series of passwords which allows them access to information and programs within their authority. Network security is controlled by Information Technology Business Unit staff and overviewed by Director, Corporate and Community

3. Breach of conditions

The conditions of this policy must be strictly adhered to. Council reserves the right to terminate use of the technology, equipment or services and to maintain that restriction at its absolute discretion if any conditions of this policy are breached.

Serious, willful or neglectful abuse or misuse of the technology or equipment by employees will result in warnings or disciplinary proceedings and may result in dismissal depending on the frequency, nature and severity of the abuse or misuse.

3.1 Indemnity by non Council personnel

The Council bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of non Council personnel in accessing or using these resources or facilities. All non Council personnel must indemnify the Council against any and all damages, costs and expenses suffered by the Council arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement.

Legal prosecution following a breach of these conditions may result independently from any action by Council.

4. Obligations of Employees

The following obligations and responsibilities apply to Employees using Council's technology, equipment and services.

4.1 Access to the systems

Formal user registration and deregistration is required.

There is a formal user registration and deregistration system that supports granting, changing or revoking access to Council's information systems in a timely way.

4.2 Personal Use

All use, personal and business, must be appropriate and lawful.

This technology is primarily for Council's business use and must be used in accordance with procedures associated with this Policy. Council recognises that a restricted and discreet use of electronic services, including telephones, may occur for private purposes. However private use must not be to the detriment of their primary use as business equipment.

4.3 Passwords and Password Confidentiality

Do not interfere with any password.

It is prohibited for anyone to:

- share their password/s with others including members of their immediate family
- hack into other systems or equipment
- read or attempt to determine the passwords of other people
- breach computer or network security measures, or
- monitor electronic files or communications of others except by explicit direction from the Leadership Team.

All electronic equipment that contains or has access to Council information must be password protected including personal mobile phones and devices which access work emails and other documents.

4.4 Identity

Email or other electronic communication must not be sent which conceals or attempts to conceal the identity of the sender.

4.5 Confidential Messages

Do not send highly confidential messages via the Internet or email.

4.6 Virus Protection

To protect the integrity and reliability of Council systems do not import non-text files or unknown messages into your system without having them scanned for viruses.

4.7 Confidentiality Clause

All documents sent or forwarded must contain Council's standard confidentiality clause.

4.8 Unlawful Activities

Do not access or send material that is prohibited or potentially prohibited, provocative, pornographic, offensive, abusive, sexist or racist. Likewise, do not forward to others any that you inadvertently receive.

4.9 Defamation

Do not be a party to or participate in the trafficking of any defamatory message or gossip.

4.10 Copyright

Be aware of copyright obligations.

Intellectual property rights apply to most material on the internet, including text, graphics and sound. Users must respect these rights.

4.11 Records Management

Emails and text messages are Council correspondence.

The corporate standards and records management requirements, practices and procedures applying to letters apply to emails text messages and any attachments.

4.12 Phone Protocol

Communication by mobile and/or fixed phones requires care and responsibility in the use of this form of communication

5. Further information

This policy will be available for inspection at the Council offices listed below during ordinary business hours and available to be downloaded, free of charge, from Council's website: www.coorong.sa.gov.au

Coorong Civic Centre	**Meningie Information Hub**	**Tintinara Customer Service Centre**
95-101 Railway Terrace Tailem Bend Phone: 1300 785 277 Fax: 8572 4399	49 Princes Highway Meningie Phone: 1300 785 277	37 Becker Terrace Tintinara Phone: 1300 785 277

Copies will be provided to interested parties upon request. Email council@coorong.sa.gov.au

Any grievances in relation to this policy or its application should be forwarded in writing addressed to the Chief Executive Officer of Council.