Electronic Communications Policy

Strategic Reference	CVP Leadership, Strategy 3.5 – Council staff and elected members act with integrity and accountability. CVP Leadership, Strategy 3.7 – Council Members demonstrate 'good governance' in their roles.
File reference	AR18/8676
Responsibility	Community & Corporate Department
Revision Number	5
Effective date	17 April 2012
Last revised date	September 2023
Minutes reference	236/23, 086/18, 069/16, 031/14, 097/12
Next review date	September 2026
Applicable Legislation	Local Government Act 1999 Freedom of Information Act 1991 State Records Act 1997
Related Policies	Behavioural Management Policy Code of Conduct Policy for Council Employees Information Security Policy Privacy Policy Records and Information 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 ensure consistency.

This Policy is fundamental to effective risk management. Standardising 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. 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. Access to data architecture will be governed through Council's Human Resources unit or the relevant Director and Chief Executive Officer.

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. This includes Council staff, Council Members, volunteers, trainees, work experience placements, independent consultants & contractors and other authorised personnel offered access to Council's resources. 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.

During a periodic election period, this policy should be read in conjunction with the Caretaker Policy.

2. Definitions

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

- World Wide Web pages
- Electronic journals and texts
- Library catalogues
- Email
- Discussion lists
- Online forums
- RSS feeds
- Internet relay chat
- Data of all kinds
- Social media
- Telephone systems, both mobile and land line
- Extranet
- Intranet
- Text messaging
- Social media/messaging apps (ie. Messenger, WhatsApp)

"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 devices. 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.

"Executive Leadership Team" comprises the Chief Executive Officer, Director Community & Corporate and Director Roads & Infrastructure.

"Extranet" – a website specifically dedicated to information sharing between Council Members and the Executive 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 the Information Technology Coordinator and overviewed by Director Community & Corporate.

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, electronic 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. These processes are administered by Information Technology and Human Resources staff in consultation with the respective manager.

Employees are required to log off correctly on a daily basis to ensure software updates can be carried out.

4.2 Personal Use

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

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.

Personal use:

- should be infrequent and brief;
- should not involve activities that might be questionable, controversial or offensive; including gambling, accessing chat lines/rooms, transmitting inappropriate jokes or sending junk programs/mail;
- must not disrupt Council electronic communication systems; and
- should not interfere with Council staff duties and responsibilities, or detrimentally affect the duties and responsibilities of other Council staff.

Council Members are not permitted to use electronic communications facilities provided by Council for a purpose that is unrelated to the performance or discharge of the respective member's official functions and/or duties. Misuse can damage Council's corporate image and intellectual property in general, and could also result in legal proceedings being brought against both Council and the user. Council staff and Council Members reasonably suspected of abusing personal use requirements will be asked to explain such use.

4.3 Passwords and Password Confidentiality

Council staff and Council Members are not permitted to 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 Executive 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.

Network administrators with privileged access rights will have the ability to establish and make changes to key servers, establish and disable user accounts and modify access levels to corporate software. Given the scale and complexity of administrator access, this will be subject to annual review as part of Council's internal financial controls and Information Technology Strategy.

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. Email systems should not be assumed to be secure, and messages are perceived to be instant in nature and instantly disposed of.

Information regarding access to Council's Information Technology and communication systems should be considered as confidential information and not be divulged without authorisation. Users are expected to treat electronic information with the same care as they would paper-based information, which is confidential. All such information should be kept secure and used only for the purpose intended. Information should not be disclosed to any unauthorised third party and it is the responsibility of the user to report any suspected security issues.

4.6 Virus Protection

Computer viruses are programs designed to make unauthorised changes to programs and data. Viruses can cause destruction of corporate resources, so 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.

Council's Information Technology Coordinator shall:

- Install and maintain appropriate antivirus software on all computers
- Respond to all virus attacks, destroy any virus detected and document each incident

All employees have a responsibility not to:

- Knowingly introduce a computer virus into Council's Information Technology network
- Load, save or open items of unknown origin

- Utilise portable media (ie. USB drive) at any point
- Attempt to solve any potential virus infection; yet ensure their workstation is switched off immediately and reported to Council's Information Technology Coordinator

4.7 Confidentiality Clause

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

4.8 Unlawful Activities

Inappropriate use includes (but is not limited to):

- use of Council's electronic communications facilities to intentionally create, store, transmit, post, communicate or access any fraudulent or offensive information, data or material including pornographic or sexually explicit material, images, text or other offensive material;
- gambling activities;
- representing personal opinions as those of Council; and
- use contrary to any legislation of any Council property.

Any Council staff member or Council Member identified as the initiator of fraudulent, unlawful or abusive calls or messages may be subject to disciplinary action.

Use of Council electronic communication facilities must not violate Federal or State legislation or common law. It is unlawful to transmit, communicate or access any material, which discriminates against, harasses or vilifies colleagues, Council Members or members of the public on the grounds of:

- gender;
- pregnancy;
- age;
- race;
- religious background;
- marital status;
- physical impairment;
- HIV status; or
- sexual preference.

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, which are classed as official records and as such, can be subject to a Freedom of Information request.

The corporate standards and records management requirements, practices and procedures applying to letters also apply to emails, text messages and any attachments. Reference should be made to Council's Records and Information Management Policy and internal procedures to properly record electronic communications.

4.12 Phone Protocol

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

5. Business Systems

Council has adopted the following primary business systems where metadata is held. This includes, but is not limited to:

5.1 Skytrust – a cloud based safety management system utilised to maintain a safe working environment for Council's staff, contractors and volunteers.

A tripartite communique between State Records of South Australia, Local Government Risk Services and Skytrust acknowledges that Skytrust is a line of a business system and as such, the information within it does not need to be transferred to a records management system. However, any outputs from Skytrust (such as reports to the Senior Leadership Team) would be subject to requirements of the General Disposal Schedule 40.

5.2 SynergySoft – a fully integrated corporate business system that encompasses key portfolios including finance, assets, cemeteries, human resources, general ledger, payroll and tenders, contracts & agreements.

5.3 Assetic – a cloud based asset management solution system which streamlines short and long term asset management.

Other web-based business systems may be deployed across Council operations to fulfil obligations such as, but not limited to, delegations management, chemical inventory, e-newsletters and external funding registers.

6. Availability/Accessibility

This Policy is available for inspection at Council's offices during normal business hours and Council's website and will be emailed to interested parties on request (please lodge request in writing via email to council@coorong.sa.gov.au).

7. Document History

This Policy will be reviewed at least every three (3) years or more frequently if legislation or Council requires.

Version	Adopted	Minute No	Description of change(s)
1	20 March 2012	097/12	New policy
2	18 February 2014	031/14	Cyclical review
3	19 April 2016	069/16	Cyclical review
4	15 May 2018	086/18	Cyclical review
5	19 September 2023	236/23	Cosmetic changes Caretaker provisions fed into policy scope Definitions enhanced Clause 4.2 – Personal Use – parameters enhanced Clause 4.5 – Confidential Messages – clause expanded Clause 4.6 – Virus Protection – clause expanded Clause 4.8 – Unlawful Activities – examples of inappropriate use provided/enhanced Clause 5 – Business Systems – new clause inserted