COPPER COAST COUNCIL	**Function:** TECHNOLOGY AND COMMUNICATIONS	Adopted: 2nd March 2022 Resolution No.: C48:0322
	Policy Number: TC005	Last Review: Resolution No.:
	Version Number: 1.1	Next Review: Annually

INFORMATION, COMMUNICATION AND CYBER SECURITY POLICY

Policy Statement

1. Introduction

1.1. The Copper Coast Council (Council) is committed to safeguarding Council infrastructure digital assets and personal information against the increasing incidence of cybercrime and espionage through implementation of the Information, Communication and Cyber Security Policy (Policy) in conjunction with the South Australian Cyber Security Framework developed by the state Government and International Organisation Standardisation (ISO27002 Compliance and ISO27002 Audit Requirements).

2. Scope

2.1. Council is aware of the significant threat different types of cybercrime and scams can cause to Council infrastructure, digital and personal information in the operation of essential services to the community.

2.2. Council will implement operating and monitoring systems to protect Councils technology and information assets from threats with the support of external cyber security specialist to assist with the management and compliance of complex and evolving threats to infrastructure digital assets and personal information.

2.3. Council will ensure all persons who have access to Council infrastructure digital assets and associated information, receive and participate in training and compliance at all times.

3. Applicable Legislation

3.1. The following legalisation applies to this Policy:

- Copyright Act 1968 (Commonwealth)
- Electronic Communications Act 2000
- Freedom of Information Act 1991
- Healthcare Act 2008
- Independent Commissioner Against Corruption Act 2012
- Information Privacy Principles Instruction (IPPI)
- Local Government (General) Regulation 2013
- Local Government (Accountability Framework) Amendment Act 2009
- Ombudsman Act 1972

- Public Interests Disclosure Act 2018
- Privacy Act 1988 (Commonwealth)
- South Australian Local Government Act 1999
- Spam Act 2003
- State Records Act 1997
- South Australian Public Health Act 2011
- Surveillance Devices Act 2016

3.2. This Policy is not a mandatory requirement but considered essential for good governance.

4. Integration with Corporate Objectives

4.1. This Policy supports Council's Strategic Plan 2019 - 2029

4.1.1. Governance Objective – Leadership

Goal 5 - To provide leadership and ensure resources are managed efficiently and effectively.

- 5.3 Legislation – To adhere to the requirements of the Local Government Act 1999, regulations and other legislation that influences the operations of Council.
- 5.6 Risk Management/Work Health and Safety Management – To ensure the effective management of all types of risk across Council's operations to minimise risks to Council, the Health and Safety of its workforce and the community.

5. Definitions

For the purposes of this Policy, the Terms of Glossary is provided on Policylite website.

6. Application

6.1. This Policy applies to Council Members, Council Employees, volunteers, trainees, work experience placements, independent consultants and other authorised personnel who act on behalf of Council or who are offered access to Council's technology and information assets.

6.2. With continuous threat to Council's technology and information assets, Council have engaged under contract an external cyber security specialist to provide:

6.2.1. An online system that supports the protection of Council infrastructure digital assets and associated information which is maintained in compliance with the SA Cyber Security Framework;

6.2.2. Council and associated persons, as listed in Clause 6.1, must undertake necessary training and adhere to requirements at all times.

6.3. This Policy is the governing Policy and must be read in conjunction with the associated information, communication and cyber security policies create to provide the protection of Councils infrastructure digital assets and associated information.

6.4. The current association policies are available on the Policylite website and are as follows:

1.	Acceptable Use Policy	Access Control, Anti-Virus, Communication & Mobile Devices, Computer Systems & Equipment Use, Email, Information Management, Internet Use, Legal Compliance, Online Services, Password & Authentication, Personnel Management, Remote Access.
2.	Access Control Policy	Privileges Granted to Users, Controlling Access to Information Systems, Preventing Unauthorised Access
3.	Anti Virus Policy	
4.	Business Continuity / DR Policy	User Participation, End User Backups
5.	Communication and Mobile Devices Policy	Acceptable Use, Mobile Devices, Bring Your Own Device, Corporate Telephone Systems, Voicemail, Voice & Video Communications
6.	Computer Systems & Equipment Use Policy	Acceptable Use of Equipment, Computer Equipment & Devices, Computer Systems & Networks, Printers & Photocopiers
7.	Computers for Councillors Policy	
8.	Cyber Crime & Security Incident Policy	Preventing Cyber Crime, Reporting Security Incidents
9.	Email Policy	Restrictions of Use, Content, Retention of Email, Rights to Privacy, Incident Management, Spam Controls
10.	Information Management Policy	Information Ownership, Management of Information, Deleting Information, Collection & Dissemination, Data Access
11.	Internet Use	Acceptable Use, Use of Social Media
12.	Laptop & Table Security Policy	
13.	Legal Compliance Policy	Confidentiality, Intellectual Property Rights & Copyright, Software Licences, Disclaimers, Misrepresentation & Defamation, Privacy, Compliance with Law
14.	Online Services Policy	
15.	Password & Authentication Policy	Password Composition, Non-Disclosure of Passwords, Password Changes, System Protection, Password Use
16.	Personnel Management Policy	Pre-Employment, During Employment, Termination Process
17.	Physical Access	
18.	Remote Access	Access Rights and Privileges, Anti-Virus & Firewall Protection, Information Management, Connection Requirements, Audit Trails & System Logs, Equipment Use.

6.5. In addition, the external cyber security will provide a complete system incorporating, but no limited to, the governing polices and the following:

6.5.1. Definitions

6.5.2. Agreements - Confidentiality Agreement, Remote Access Agreement for Third Parties

6.5.3. Procedures - Handling a Security Incident

6.5.4. Forms - Acceptable Use Policy Sign Off, Change/Remove Computer Access Request Form, Councillors Equipment Loan Form, Incident Report Form, Laptop and Table Custodian Form, Loan Equipment Form, New Computer Initiative Form, New Hardware or Software Request Form, New User Computer Access Form, Remote Access Application Form for Third Parties, Request for Change Form, Security Check Form, Server Health Check List, Staff Remove Access Request Form, User Termination Request Form

6.5.5. Guides and Training Videos.

7. Delegation

7.1. Pursuant to section 44 of the Local Government Act 1999, Council delegates to the Chief Executive Officer authority to administer Council's policies.

7.2. The Policy implement and compliance is delegate to the Information Community Technology Services Coordinator

8. Adoption and Review

8.1. This Policy shall be reviewed annually, or more frequently, if legislation or Council requires by the Information Community Technology Department and a report shall provide to Council for consideration and adoption.

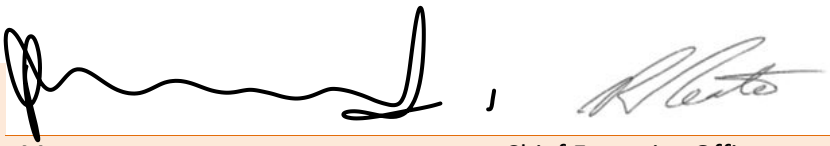
9. Records Management

9.1. Official records will be retained and stored in accordance with Council's adopted Records Management Policy as required by section 125 of the Local Government Act 1999.

10. Availability of Policy

10.1. This Policy and associated documents, as listed, will be available for inspection without charge at the Council's Principal Office during normal business hours and via the Council's website www.coppercoast.sa.gov.au.

10.2. A copy of this Policy may be obtained on payment of a fee in accordance with Councils' Schedule of Fees and Charges.

Signed		
	Mayor	Chief Executive Officer
Date		