

# 2209 Digital Information and Communications Technology (ICT)

## Governance Policy



### PURPOSE

- 1) Council is committed to improving services for the community, by better use and analysis of digital information, and by using modern, cost-effective technologies.
- 2) To support and achieve this commitment, Council is dedicated to maintaining an ICT framework for the effective management of information, and technology. In turn, ensuring ICT systems are controlled and maintained in line with both corporate objectives and emerging trends.

### SCOPE

- 3) This policy applies to all digital information and information assets supporting Information and Communications Technology (ICT) assets that are owned, managed, or operated by Council.
- 4) This Policy applies to the use of Council's ICT systems by Councillors and employees.

### DEFINITIONS

Term	Definition
Information	A collection of data or documents processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium (including electronic (digital), print, audio, video, image or graphical form).
Information Asset	A collection of data stored in any manner and recognised as having value for the purpose of enabling the Council to perform its business functions, thereby satisfying a recognised Council requirement.
Employee	Includes all Council employees, regardless of their employment status, role or position - permanent, temporary, or part-time basis and includes volunteers and employees of businesses and entities contracted to provide services to, or on behalf of Council.
ICT	ICT means Information and Communications Technology and includes: <ul style="list-style-type: none"><li>• equipment and facilities,</li><li>• networks and devices connected to those networks,</li><li>• servers</li><li>• desktop computers and laptops,</li><li>• mobile devices,</li><li>• communications infrastructure and services,</li><li>• cloud infrastructure (including Software as a Service),</li><li>• Internet of Things infrastructure,</li><li>• printers,</li><li>• operating systems and software.</li></ul>
Intolerable Risk	A level of risk which cannot be tolerated. See Corporate Risk – Consequence & Likelihood Table, Risk Matrix

### POLICY

- 5) Council's ICT systems must only be used for carrying out official Council business in accordance with any supporting Procedure or Directive.
- 6) Personal information may be collected through use of an ICT asset and that information will be dealt with in accordance with the *Information Privacy Act 2009*, Information Privacy Principles and Councils Information Privacy Policy.

## OBJECTIVES

- 7) Innovation is embraced and recognised as a key enabler in driving productivity through new ways of delivering services to:
  - Deliver strategically aligned solutions in accordance with Council's Corporate Plan;
  - Align Council's ICT architecture and plans with business priorities and ensuring ICT resources are deployed appropriately to fulfil approved demand for ICT services;
  - Deliver ICT services that provide sustainable value to the business by maximising benefits and minimising delivery risk;
  - Follow appropriate governance practices to ensure consistent and efficient service delivery;
  - Establish controls to ensure that Council's digital information is effectively managed to maintain appropriate confidentiality, integrity and access;
  - Ensure ICT assets and their interrelationships are appropriately managed throughout their service lifecycle;
  - Ensure ICT services are designed, maintained, and delivered in accordance with best practice service levels.

## POLICY STATEMENT

- 8) Council is committed to ensuring the provision and availability of ICT services to efficiently perform Council functions and improve the effectiveness with which Council serves the community.
- 9) Council's ICT framework will facilitate a cultural shift in the organisation from being process-oriented to customer-centric.
- 10) The use of ICT systems is an integral part of Council's daily operations. Council is committed to the appropriate use of ICT systems by Councillors and employees in accordance with relevant legislation and Council's corporate values.
- 11) Failure to comply with this Policy or supporting procedures or directives may result in disciplinary action or for appropriate offences or breaches, referral to law enforcement for investigation or prosecution.

## ROLES AND RESPONSIBILITIES

- 12) All Councillors and employees must not disclose information that they know, or should reasonably know, is confidential by any means.
- 13) All Councillors and employees have an obligation to report digital information security breaches or suspected digital information security breaches.
- 14) Security incident management responsibilities and procedures must be established by employees responsible for information assets. This is to ensure an effective and efficient response to information security incidents in accordance with the Information Security Incident Management Standard (ISO 27001 - Annex A.16).
- 15) Council must operate an Information Security Management System (ISMS) to provide a systematic and repeatable approach to minimising information security risks, support cyber resilience and reduce the impact of security incidents.
- 16) Employees responsible for information assets must identify information security risks in accordance with the Information Security Risk Management Standard (ISO/IEC 27005:2018).

## APPLICABLE LEGISLATION AND REGULATION

- 17) Applicable legislation and regulation:
  - *Crime and Misconduct Act 2001*
  - *Electronic Transactions (Queensland) Act 2001*
  - *Evidence Act 1997*
  - *Information Privacy Act 2009*
  - *Local Government Act 2009*
  - *Public Records Act 2002*
  - *Right to Information Act 2009*
  - *Cybercrime Act 2001*
  - *Spam Act 2003*
  - *Telecommunication Act 1997*
  - *Security of Critical Infrastructure Act 2018*

## RELATED DOCUMENTS

- 18) Related documents are:
- a) NBRC Code of Conduct
  - b) Digital Information and Communications Technology (ICT) Procedures

## RESPONSIBLE OFFICER

General Manager Corporate and Community

## APPROVAL DATE

19 July 2021

## REVIEW DATE

July 2025 (Standard four year term)

## REVISION HISTORY

Version	General Managers	Approval Date	History
1	General Manager Corporate and Community	19 July 2021	New