ICT Security

1. Purpose

Glenorchy City Council (Council) is committed to safeguarding the confidentiality, integrity and availability of information and technology assets that enable services to our community. This policy states Council's strategic intent and governance approach to ICT security.

2. Scope

This policy applies to Council information, ICT assets and environments owned, contracted or otherwise controlled by or for Council, and to all individuals authorised to access Council systems, including Elected Members and external parties engaged by Council.

Statutory Requirements

Acts	*Privacy Act 1988* *Cyber Security Act 2024* *Criminal Code Act 1995 – Computer Offences* *Personal Information Protection Act 2004 (Tas)* *Local Government Act 1993 (Tas)*
Regulations	N/A
Policy	Alderman Code of Conduct Policy ICT Acceptable Use Guidelines Directive Information Management Policy Open Data Policy Privacy Policy Risk Management Policy

Definitions

Corporate Systems – Are defined as all technology resources, including hardware, software, data, and networks, that are owned, contracted, or otherwise controlled by or for Council and used to conduct its business operations.

Device – Any Council-owned or approved hardware used to access Council information or systems.

ICT – Means Information, Communications and Technology.

User – Is a person authorised to use Council owned devices and / or Council systems. This includes but not limited to staff members, consultants, contractors, volunteers and vendors.

Personal Information – Refers to any data that can be used to identify an individual (commonly referred to as Personally Identifiable Information or PII), such as names, Centrelink numbers, bank account details, email addresses, etc., as defined in the Personal Information Protection Act 2004.

Security Principles

Risk based protection: Security controls are selected and applied proportionately to the sensitivity of information and the risks to Council and the community.

Confidentiality, Integrity, Availability: Council safeguards information from unauthorised access or disclosure, prevents unauthorised alteration or destruction, and promotes reliable access for authorised purposes.

Least privilege and need to know: Access is limited to what is necessary for legitimate business needs and is reviewed periodically.

Accountability: Security is everyone's responsibility. Users must understand and meet their obligations.

Continuous improvement: Policies and internal directives are reviewed regularly to remain effective against evolving threats and to align with organisational objectives.

Policy Statement

Governance and Accountability

- Council will maintain an enterprise ICT security approach that is risk-based, proportionate, and aligned with applicable legislation and relevant standards.
- Council requires the Chief Executive Officer is to establish, implement and maintain ICT security directives, procedures and supporting instruments to give effect to this policy, and to ensure appropriate resources, assurance and reporting are in place.

Roles

- Elected Members agree to comply with the approved directives and procedures and other related instruments in their use of Council information and systems.
- The Chief Executive Officer is responsible for implementing this policy through approved directives and procedures, maintaining capability (people, process and technology), and ensuring continuous improvement and compliance.

Risk Management and Resilience

- Council will identify and assess ICT and cyber risks, taking steps to reduce the likelihood and impact of incidents consistent with its risk appetite and community service obligations.
- Council will maintain arrangements that support business continuity and disaster recovery for critical services.

Information Protection and Privacy

- Council will protect personal, sensitive and corporate information and ensure that privacy and recordkeeping obligations are met.

Security Awareness

- Council will ensure a security awareness and education program is maintained so that authorised users understand their responsibilities and evolving threats.

Third-Party and Cloud Assurance

- Council will ensure that contracts and procurement processes incorporate appropriate ICT security, privacy and data handling requirements, with proportionate assurance and monitoring of third parties.

Compliance and Assurance

- Council requires compliance with this policy, the ICT Acceptable Use Guidelines Directive and associated procedures.
- The Chief Executive Officer will ensure appropriate monitoring, reporting and review mechanisms are in place, and will escalate notifiable incidents to the relevant authorities as required by law.

Non-Compliance

- Anyone found to have breached this policy may be subject to investigation and disciplinary action in accordance with relevant Council directives, policies and codes of conduct.

Implementation Responsibility

The Chief Executive Officer is responsible for implementing this policy by ensuring that ICT security directives, procedures and supporting instruments are developed, maintained and applied. These instruments contain the operational requirements necessary to give effect to Council's strategic intent and may be updated as required without amendment to this policy.

COUNCIL POLICY

Version Control

VERSION	Item 2.0	**ADOPTED**	30 March 2026	**COMMENCEMENT DATE**	31 March 2026
MINUTES REFERENCE	Item 11.1			**REVIEW PERIOD**	4 Years from adoption
PREVIOUS VERSIONS	V 1.0 adopted 26 October 2020 (Council meeting, Item 14)				
RESPONSIBLE DIRECTORATE	Corporate and Community Services	**CONTROLLER**	Manager ICT		
ECM DOCUMENT NO	Policies by Directorate				