Information Communication Technology (ICT) Acceptable Use Policy

Yarriambiack
SHIRE COUNCIL

Information Communication Technology (ICT) Acceptable Use Policy

Yarriambiack Shire Council encourages a working environment which promotes gender equality and models non-violent and respectful relationships.

Contents

Information Communication Technology (ICT) Acceptable Use Policy

Yarriambiack Shire Council encourages a working environment which promotes gender equality and models non-violent and respectful relationships.

1 Objective

This policy establishes a governance framework for the appropriate, secure and efficient use of Council ICT resources. It aims to:

a) Ensure ICT resources support Council business activities and service delivery

b) Minimise operational, security and reputational risks

c) Promote responsible, ethical and lawful use of ICT resources

d) Ensure compliance with legislation, policies and governance obligations

2 Scope and Responsibilities

This policy applies to all users who access, use or manage Council ICT resources, including:

a) Employees

b) Councillors

c) Contractors and consultants

d) Third parties authorised to access Council ICT systems

e) Volunteers and labour-hire personnel where access to Council ICT resources is authorised

2.1 Roles and accountability

a) The Chief Executive Officer and Executive Leadership Team are responsible for ensuring the policy is implemented, appropriately resourced and monitored.

b) The Manager Business Systems is responsible for maintaining ICT controls, providing advice, monitoring security risks and coordinating responses to ICT incidents.

c) The Department of People and Culture will support onboarding, offboarding, training, disciplinary processes and recordkeeping relating to employee compliance with this policy.

d) Managers and supervisors are responsible for ensuring users understand and comply with this policy, complete required training and promptly report suspected breaches.

e) All users are responsible for complying with this policy, protecting Council information and using ICT resources lawfully, ethically and professionally.

2.2 User Security Responsibilities include:

a) Protect credentials and not bypass security controls (e.g. MFA)

b) Lock devices when unattended

c) Report suspicious activity including suspicious emails or messages (e.g. phishing)

d) Use only approved systems and configurations

e) Report any suspected information breaches or cyber security incidents

3 Policy Statement and Scope

3.1 Scope of ICT Resources

ICT resources include all Council owned or managed systems and devices, including:

a) Computers, laptops, mobile devices

b) Networks, internet and email systems
c) Software and applications
d) Telecommunications systems, equipment and collaboration platforms
e) Data storage systems and platforms
f) Cloud services, artificial intelligence tools, and digital records

Use of these resources is permitted for official business purposes, with limited personal use permitted under defined conditions.

3.2 Principles of Acceptable Use

All use of Council ICT resources must:

a) Support Council operations and objectives
b) Be lawful, ethical and consistent with Council values
c) Protect information security, privacy and confidentiality
d) Withstand public scrutiny and audit review
e) Comply with Council policies and relevant legislation

3.3 Authorised Use

Use directly related to Council business, including:

a) Performing work duties
b) Accessing business information
c) Communicating internally and externally on Council matters
d) Training, study or conferences
e) Participation in professional networks
f) Accessing industry related resources

3.4 Limited Personal Use

Permitted where it:

a) Is minimal and occurs in personal time
b) Does not impact operations or incur cost
c) Does not breach policy or legislation
d) Does not involve private business or personal gain
e) Can withstand public scrutiny

3.5 Prohibited Use

Users must not use ICT resources for activities that:

a) Are unlawful, unethical or in breach of legislation
b) Involve offensive, inappropriate or harmful material
c) Harass, bully or discriminate against others
d) Avoid security or governance controls
e) Create risk or burden to Council systems
f) Support private business or personal profit
g) Misrepresent Council, exceed delegated authority or disclose confidential information without authorisation

Serious breaches may result in disciplinary action or legal consequences.

3.6 Information Management and Security

All information must be handled in accordance with its classification and risk:

a) Sensitive, personal or confidential information must only be accessed, used or shared where there is a legitimate business need and appropriate authority.

b) Council information must be stored in approved systems and managed in accordance with Council recordkeeping requirements.

c) Information must be protected against loss, misuse, unauthorised access, unauthorised disclosure or inappropriate deletion.

d) Information must be managed in accordance with privacy, public records, audit and information security obligations.

4 Data Privacy, Confidentiality and Intellectual Property

Council information, records, data, documents, systems, content and intellectual property created, stored, accessed or transmitted using Council ICT resources remain Council assets unless otherwise agreed in writing.

a) Users must only access, use or disclose Council information where there is a genuine business need and appropriate authority.

b) Confidential, personal, health, financial, commercial or security-sensitive information must be handled securely and in accordance with Council privacy, records management and information security obligations.

c) Council information must only be stored, shared or transferred using approved systems, platforms and file sharing methods.

d) Users must not copy, export, reuse, publish or disclose Council intellectual property or confidential information externally without appropriate authorisation.

e) Actual or suspected privacy breaches, unauthorised disclosures or inappropriate access to Council information must be reported immediately.

5 Monitoring and Compliance

Council may monitor ICT usage to:

a) Maintain system security and performance

b) Ensure compliance with legal and policy obligations

c) Support audit, incident response and investigations

Monitoring will be proportionate, authorised and conducted in accordance with privacy, employment and recordkeeping obligations.

5.1 Technology Specific Use Requirements

Internet and Email

a) Council email is part of corporate records and subject to monitoring

b) Users must not send spam, chain mail or inappropriate content

global emails require approval from the CEO, COO, CFO, CengO or CPCO. Only authorised staff can send our global emails

Microsoft 365 and Digital Environment

a) Only approved systems and access methods may be used

b) Devices must be always secured

c) Systems must be used efficiently and sustainably, including powering down devices when appropriate.

Artificial Intelligence (AI)

a) Must only be used where approved

b) Must not be used to upload, disclose or expose confidential, personal, sensitive or security classified information unless expressly approved and appropriately controlled

c) Outputs must be reviewed and validated

d) Human review and accountability are required for any AI assisted output or decision that may impact Council operations, employees, customers or the community

e) Use of AI systems must comply with Council's Use of Artificial Intelligence Policy.

5.2 Devices and Telecommunications

a) Use must align with operational purpose

b) Personal use is restricted

c) High cost or external services require approval by COO or CEO

d) Users may be liable for negligent loss or damage

e) Users must take reasonable care of Council issued ICT assets and must secure devices when not in use, including during travel, remote work or off site duties.

f) Lost, stolen, damaged or malfunctioning ICT assets must be reported to the Manager Business Systems or team members as soon as possible.

g) All Council issued ICT assets, accessories, access cards, authentication devices, passwords or passcodes must be returned when employment, engagement or authorised access ends, or earlier if requested by Council.

h) Council may seek recovery of repair or replacement costs where loss, damage or misuse results from wilful misconduct, gross negligence, unauthorised modification or failure to comply with reasonable care requirements.

5.3 Software and Applications

a) Only authorised software may be installed

b) Licensing conditions must be adhered to

c) Downloads from external sources are prohibited unless approved

5.4 Remote Access and Bring Your Own Devices

a) Access must be authorised and secure

b) Personal devices must comply with Council controls

c) Council information must not be stored or shared inappropriately

d) Access may be restricted or revoked at any time

6 Training and Awareness

Users must complete any mandatory ICT security, privacy, records management, cyber awareness, artificial intelligence or related training required by Council. Managers and supervisors are responsible for ensuring relevant users complete required training and understand their obligations under this Policy.

7 Policy Exemptions

Any exception to this Policy must be approved by the Manager Business Systems, Chief Operating Officer or the Chief Executive Officer. Exemptions must be documented, include the reason for the exception, identify any associated risks or controls, be time limited where appropriate, and be reviewed periodically.

8 Breaches and Enforcement

a) All suspected breaches must be reported

b) Council will investigate and take appropriate action

c) Breaches may result in disciplinary, contractual or legal consequences

Examples of reportable ICT or information security incidents include, but are not limited to:

- Phishing emails, suspicious links, scam messages or suspected credential compromise.
- Malware, virus alerts, ransomware, cyber extortion or other malicious activity.
- Unauthorised access to Council systems, accounts, files or information.
- Lost, stolen, damaged or tampered devices, access cards or authentication tools.
- Accidental disclosure of information, including sending information to an incorrect recipient.
- Unauthorised installation of software, applications, browser extensions or cloud services.
- Any actual or suspected privacy breach, data loss or inappropriate disclosure of Council information.

9 References

a) Information Privacy Policy
b) Employee Code of Conduct
c) Councillor Code of Conduct
d) Mobile Phone Policy and Procedure
e) Human Resource Policy and Guidelines Manual
f) Use of Artificial Intelligence Policy
g) Privacy and Data Protection Policy and Records Management procedures

10 Contact Information

For advice or guidance about this Policy, users should contact their Line Manager, the Manager Business Systems, People and Culture, or Business systems team.

11 Definitions

Term	Description
ICT Resources	All Council owned, leased, managed or authorised information and communication technology assets, services and systems, including devices, networks, software, applications, cloud services, telecommunications, data storage platforms and digital information.
User	Any employee, contractor, consultant, volunteer, Councillor or other authorised individual who accesses, uses or manages Council ICT resources.
Malware	Malicious software or code designed to disrupt operations, gain unauthorised access, damage systems, compromise security, or steal, alter or destroy information.
Personal Use	Limited use of Council ICT resources for personal purposes that is infrequent, does not interfere with work duties, does not incur

	additional cost to Council, and complies with this Policy and relevant legislation.
Council Information	Any information created, received, stored, processed or transmitted by Council in any format, including records, emails, documents, images, data, correspondence and information relating to Council business.
Artificial Intelligence (AI)	Technology that can generate, analyse or process content, information, images, code or data using machine learning or other computational techniques. This includes generative AI tools such as Microsoft Copilot, ChatGPT, Claude and similar technologies.
Approved Systems	ICT systems, software, applications, cloud services, platforms and devices that have been authorised by Council for business use and are managed in accordance with Council security, governance and operational requirements.
BYOD (Bring Your Own Device)	A personally owned device, such as a mobile phone, tablet or computer, that is authorised for access to Council information, systems or services subject to Council security and management requirements.
Cyber Security Incident	Any actual or suspected event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of Council information, systems or services. This includes phishing attacks, malware infections, unauthorised access, data breaches and other security events.
Confidential Information	Information that is not publicly available and requires protection from unauthorised access, use or disclosure due to legal, privacy, commercial, security or operational considerations.
Personal Information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information.
Sensitive Information	Information that requires a higher level of protection because of its nature, including information relating to health, financial circumstances, employment, identity, security, legal matters or other confidential Council business.
Policy Breach	Any act, omission or conduct that does not comply with this Policy, associated procedures, lawful directions, approved ICT controls, or Council's information security, privacy or recordkeeping requirements.

12 Consistency with Governance Principles Local Government Act 2020

This policy supports governance principles by:

Governance Principle	Section of policy where covered
a) Council decisions are to be made and actions taken in accordance with the relevant law;	Section 15 - Legislative Context

Governance Principle	Section of policy where covered
b) priority is to be given to achieving the best outcomes for the municipal community, including future generations;	Section 3 - Policy Statement and Scope
c) the economic, social and environmental sustainability of the municipal district, including mitigation and planning for climate change risks, is to be promoted;	Section 3 - Policy Statement and Scope
d) the municipal community is to be engaged in strategic planning and strategic decision making;	Not Applicable
e) innovation and continuous improvement is to be pursued;	Section 3 - Policy Statement and Scope
f) collaboration with other Councils and Governments and statutory bodies is to be sought;	Section 14 - Collaboration
g) the ongoing financial viability of the Council is to be ensured;	Section 3 - Policy Statement and Scope
h) regional, state and national plans and policies are to be considered in strategic planning and decision making;	Section 15 - Legislative Context
i) the transparency of Council decisions, actions and information is to be ensured.	Section 3 - Policy Statement and Scope

In giving effect to the overarching governance principles, a Council must take into account the following supporting principles.

Community Engagement Principles	• A community engagement process must have a clearly defined objective and scope. • Participants in community engagement must have access to objective, relevant and timely information to inform their participation. • Participants in community engagement must be representative of the persons and groups affected by the matter that is the subject of the community engagement. • Participants in community engagement are entitled to reasonable support to enable meaningful and informed engagement. • Participants in community engagement are informed of the ways in which the community engagement process will influence Council decision making.
Comment:	*Not Applicable*

Public Transparency Principles	• Council decision making processes must be transparent except when the Council is dealing with information that is confidential by virtue of this Act or any other Act. • Council information must be publicly available unless— (i) the information is confidential by virtue of this Act or any other Act; or (ii) public availability of the information would be contrary to the public interest. • Council information must be understandable and accessible to members of the community. • Public awareness of the availability of Council information must be facilitated.
Comment:	*This policy supports transparency through requirements relating to information management, recordkeeping, audit, monitoring and the lawful use of Council ICT resources.*
Strategic Planning Principles	• An integrated approach to planning, monitoring and performance reporting is to be adopted. • Strategic planning must address the Community Vision. • Strategic planning must take into account the resources needed for effective implementation. • Strategic planning must identify and address the risks to effective implementation. • Strategic planning must provide for ongoing monitoring of progress and regular reviews to identify and address changing circumstances.
Comment:	*Not Applicable*
Financial Management Principles	• Revenue, expenses, assets, liabilities, investments and financial transactions must be managed in accordance with a Council's financial policies and strategic plans. • Financial risks must be monitored and managed prudently having regard to economic circumstances. • Financial policies and strategic plans, including the Revenue and Rating Plan, must seek to provide stability and predictability in the financial impact on the municipal community. • Accounts and records that explain the financial operations and financial position of the Council must be kept.
Comment:	*The policy promotes the responsible, secure and efficient use of Council ICT resources, helping to minimise financial, operational and security risks.*

Service Performance Principles	• Services should be provided in an equitable manner and be responsive to the diverse needs of the municipal community. • Services should be accessible to the members of the municipal community for whom the services are intended. • Quality and costs standards for services set by the Council should provide good value to the municipal community. • A Council should seek to continuously improve service delivery to the municipal community in response to performance monitoring. • Service delivery must include a fair and effective process for considering and responding to complaints about service provision.
Comment:	*This policy supports the reliable and secure operation of ICT resources that enable the delivery of Council services to the community.*

13 Policy Review

This policy will be reviewed in conjunction with its associated procedures every three years.

From time to time, circumstances may require minor administrative changes to be made to this Policy. Where an update does not materially alter this Policy, such a change may be made administratively and need not be considered and adopted by Council.

Where any change or update may materially change the intent of this policy, or the legal responsibilities of any member of the community, it must be considered and adopted by Council, or by the Chief Executive Officer in reliance on delegated authority.

14 Collaboration

Council will collaborate, where practical, with other Councils, Governments and statutory bodies when implementing this policy and associated provisions.

15 Legislative Context

This Policy supports Council's obligation to give effect to the overarching governance principles by establishing clear expectations for the secure, lawful and responsible use of ICT resources.

Related *Acts*:

a) *Privacy and Data Protection Act 2014*

b) *Victorian Protective Data Security Act 2013*

c) *Public Records Act 1973*

d) *Local Government Act 2020*

Council Approved Policy

Adopted:	Ordinary Council Meeting 24 June 2020	Minute Page 157
Reviewed:	Ordinary Council Meeting 23 August 2023	Minute Page 32
	Ordinary Council Meeting 26 August 2023	Item [number] Minute Page [number]