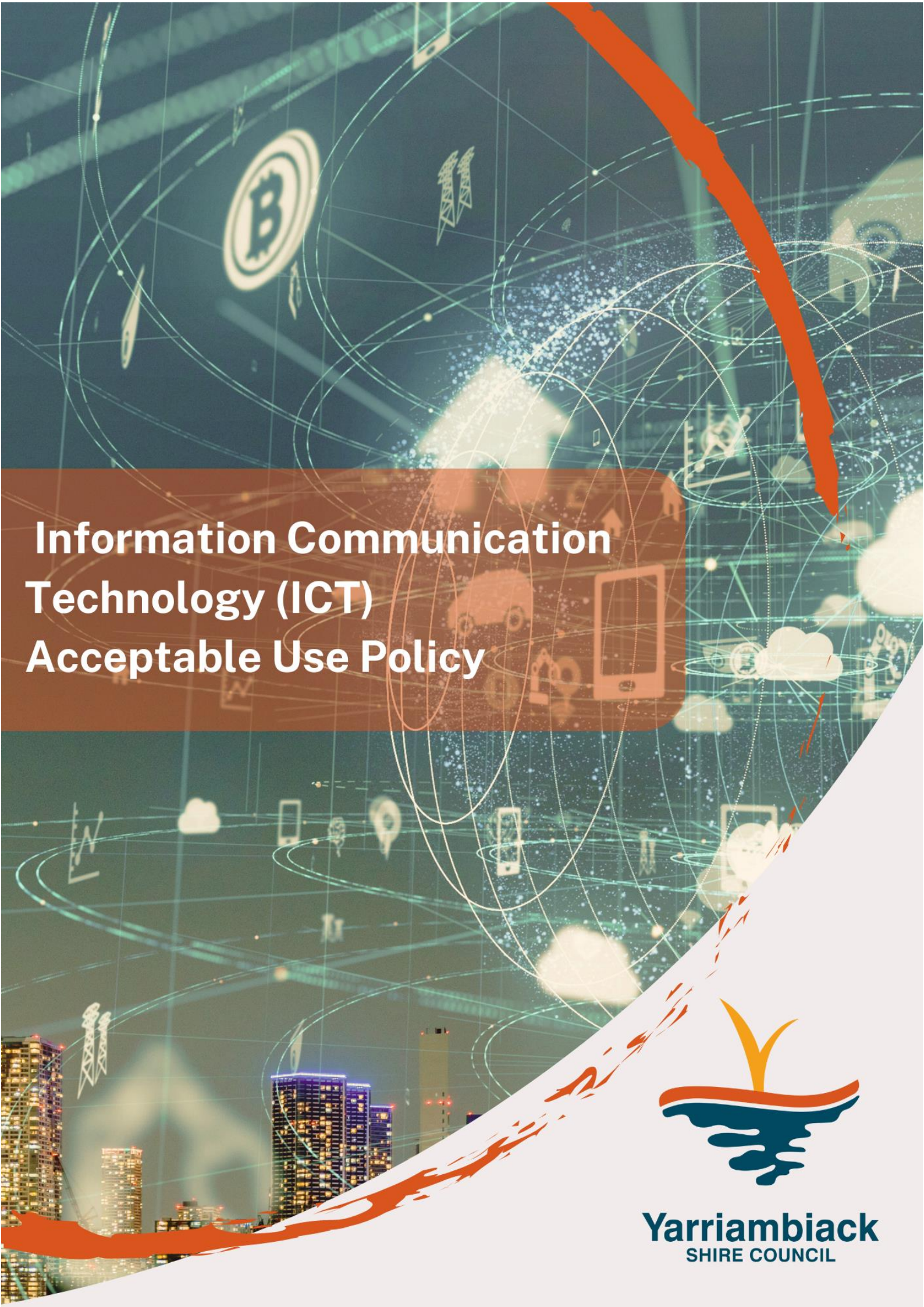

Information Communication Technology (ICT) Acceptable Use Policy

Yarriambiack
SHIRE COUNCIL

ICT Acceptable Use Policy

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

Contents

Definitions

Authorised Officers - Staff within Yarriambiack Shire Council performing duties authorised by management.

Call Diversion - An automatic diversion of a call from the called extension to another number.

Chain Mail - An email directing recipients to send out multiple copies of it so its circulation increases exponentially. Such messages typically promise rewards for compliance, e.g. blessings, good luck, money or merchandise. Some types of chain letters - specifically, those asking people to send money to other participants - are illegal and not in accordance with Council policy.

Corporate Information - Corporate information refers to all records and their associated contextual information that serves to completely depict all details of a particular business activity and its relationship to other business activities.

Corporate Memory - A full and accurate record of all the business activities and transactions undertaken by Council in the exercise of its statutory, administrative or other public responsibilities or related purposes.

Council – Yarriambiack Shire Council

Councillors - Councillors refer to all elected officials in Council including Councillors and Mayor.

Download - A mechanism by which a software device, program or file is copied from a one location to another, typically over the internet.

Electronic Correspondence - Any correspondence facilitated by ICT resources.

Email - The transmission of messages, and attachments in electronic format to an address within an email system.

Email System - A software application that provides services related to the transmission and receipt of electronic messages.

End-user Devices - End-user devices are defined as Standard desktop computer, Standard notebook (portable) computer, various computer (PC) models, other mobile computing devices, printers, smart phones etc.

Excluded Call Types - Call types which are not included in Council's current mobile phone contract access fee and for which additional charges are payable.

External Entity - An independent organisation with which Council has a contractual arrangement and which is provided with equipment that is serviced by Council.

Global Email - Email communications that are sent out to the entire organisation. Such email must be authorised by a Manager.

ICT Resources - ICT resources include but is not limited to:

- Computers (including laptops, notebooks, tablets);
- Electronic storage devices;
- Telecommunications (including provisioned phone lines/connections, telephones, mobile phones, pagers, facsimiles, message banks, voice mail, modems, data communication devices and data cabling);
- Radios (or any other frequency devices);
- Television sets (including LCD and plasma screens);
- Video and imaging equipment;
- Digital or analogue recording devices (including tape, DVD, video recorders);
- Cameras (including mobile phones with cameras);

- Printers, copiers and digital scanners;
- Internet services (including http, ftp and telnet, peer to peer, video-streaming);
- Email services;
- Web based portals; and
- Fee based services.

Internet - The worldwide loose affiliation of interconnected computer systems, through which users can navigate to obtain services and share information at various levels of detail with globally dispersed organisations and individuals.

Malicious Software (Malware) - Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

Peripheral Device - A device that is optional in nature, and is attachable to an end-user device e.g. USB Drives, external hard drives, scanners and cameras.

Programmable Devices - Any device whose operation is controlled by a stored program that can be changed or replaced. Information may comprise automated software, data files and temporary work files. Such devices would include desktop computers, mobile communications devices etc.

SPAM - An unsolicited message that is sent indiscriminately to multiple mailing destinations.

Tethering/Tethered - Connecting a data-enabled mobile telephone or tablet device to a computer or other device via a cable or wireless connection for the purpose of connecting to the Internet via the phone/tablets' data connection.

User - Any authorised Council staff member, Councillor, contractor or third party.

Virus - A software agent that uses any programmable device that is available to reproduce itself and spread itself to other programmable devices.

Voice Mail - The ability to store a message for an extension that can be replayed at a later time.

Information Communication Technology Acceptable Use Policy

1. Objective

Yarriambiack Shire Council's Information, Communication and Technology (ICT) resources are to be used in an ethical and efficient manner within a sound governance framework, thereby enabling Council's assets to be appropriately managed within acceptable risk tolerances. A key underpinning goal of this approach is to ensure users of ICT resources behave in ways that support the business activities and objectives of Council.

This policy aims to ensure that Council's ICT resources are used:

a) Appropriately and efficiently.

b) To assist Council to effectively deliver quality, value for money services.

c) To not create or increase risk to Council, Council employees, Councillors, Contractors and third parties.

d) In accordance with other policies, legislation, standards and best business practices.

e) Managed with sound consistent governance across Council.

2. Responsibility

This Policy applies to all Council employees, consultants, Councillors, contracted external staff, patrons and or service providers.

It is the responsibility of the Chief Executive Officer (CEO), Chief Operating Officer (COO) and Managers to ensure compliance with this Policy.

3. Policy Statement and Scope

3.1 ICT Resources

The provision of Council owned ICT resources are to be used for officially approved purposes only. Limited personal use of ICT resources is available only in accordance with the uses outlined in this Policy and supporting Procedures.

Council employees, consultants, contracted external service providers and Councillors are all required to use Council ICT resources in accordance with this Policy, associated Procedures and Employee and Councillor Code of Conduct.

All access to ICT resources is granted on the basis of business need and may be revoked at Management discretion.

All ICT resource users must be aware of:

a) Types of ICT resources.

b) Authorised, unauthorised and unlawful/criminal use of Council resources.

c) Business rules regarding use of each resource.

Serious breaches of this Policy and associated Procedures will be referred to the applicable Manager for consideration and action taken in accordance with the Human Resource Policy and Guidelines Manual.

3.2 Council Responsibilities

The provision of Council ICT resources is for officially approved purposes. When managing and monitoring the use of ICT resources, Council must:

a) Ensure users are aware and understand Council Policies, Procedures, Practices and their responsibilities.

b) Ensure disciplinary procedures imposed on users for breaches of use are clear, unambiguous, proportionate to the offence and are applied in a manner which is in accordance with the principles of natural justice.

c) Ensure that employees are aware that intentionally accessing, downloading, storing or distributing pornography or other material which could be reasonably expected to cause offence, or breaches the principles contained in the Employee Code of Conduct is a matter for which disciplinary action is taken.

d) Minimise security risks including disruption to Council operations and unauthorised use (intentional or unintentional) by employees.

e) Address issues relating to record keeping, archiving, right to information, privacy and audit requirements.

f) Ensure any breaches discovered are thoroughly investigated and all issues identified and addressed.

g) Develop and implement procedures for reporting potential breaches of Council policy or the law to relevant authorities.

h) Ensure that sufficient resources are made available for the above to be carried out effectively.

3.3 Authorised Use of ICT Resources

The Council's ICT resources are:

a) Provided to Councillors, staff and contractors to conduct official business and professional development more effectively and efficiently.

b) To be utilised only for defined use outlined in this policy.

c) To be authorised by the relevant Manager, COO or CEO and used in accordance with Council policies and procedures, applicable laws and regulations.

d) Provided to employees and Councillors and able to survive public scrutiny and/or disclosure.

e) Not to be used to bypass established and/or official channels of communication as defined by Council reporting relationships.

f) Staff laptops are logged by the ICT Managed Service Provider in accordance with Council's Policies and Procedures and under the supervision of the COO. Other ICT equipment and devices are logged in Happy HR or AssetFinda systems.

g) Subject to the Council's recordkeeping, archiving, right to information, information privacy and auditing requirements.

h) Able to be restricted or revoked at any time.

Authorised Official Use

Official use of Council owned or provided ICT resources means usage undertaken for a business need to assist in carrying out the work of Council.

Official use includes in general:

a) Conducting work related business.

b) Access to work related information.

c) Communication with colleagues on work related matters.

d) Communication outside the work environment on work related matters.

Official use is permitted under the following conditions and limitations:

a) Usage takes place while you are either employed, contracted or are an elected official in the service of Council.

b) Established and/or official channels of communication as defined by Council reporting relationships are observed at all times.

c) Usage that could interfere with day-to-day operations must receive the appropriate authorisation from the relevant Manager.

Examples of Official Use include, but are not limited to:

a) Phoning other Government agencies for the purpose of acquiring or sharing information.

b) Printing documents relating to a Council training course.

c) Using the Internet to perform Council related case/project research.

d) Using email to communicate new Council directives or policies.

e) Informing employees of new Council initiatives and/or staff movements.

Authorised Professional Use

Professional use of Council owned or provided ICT resources means permitted activities that support professional development with authority from the relevant Manager.

Professional use includes in general:

a) Professional development relating to approved study or research.

b) Approved forum, conference or seminar participation.

c) To engage with a professional or industrial organisation for membership, registration, training/education, performance, conduct or safety.

d) Council approved or supported personal study.

Professional use is permitted under the following conditions and limitations:

a) Usage has been authorised by the COO.

b) Established and/or official channels of communication as defined by Council reporting relationships are observed at all times.

c) Use does not threaten or interfere with day-to-day operations of the Council in accordance with ethical standards explained in Council's Code of Conduct for employees or Councillors.

d) Unnecessary or excessive burden is not placed on Council resources, e.g., large-scale emailing or mass storage or transmission of electronic files.

e) Access does not require modifications to existing infrastructure.

Examples of Professional Use include, but are not limited to:

a) Using the Internet/email to book and confirm a professional membership seminar/conference.

b) Enabling staff to access information from their professional bodies website.

c) Using a facsimile to apply for professional body membership.

d) Printing and distributing information relating to professional training / conference / seminar events.

e) Enabling third parties to call professional bodies for advice when working for Council.

Authorised Limited Personal Use

Limited use of Council owned or provided ICT resources means those activities conducted for purposes other than official business or professional development.

Users who have been issued with a mobile device such as an tablet, mobile phone or laptop have been allocated with that specific device and as such it is the responsibility of that user. The user must be mindful that although some limited personal use is authorised, such devices can be reallocated for operational purposes to another user.

Limited use is permitted under the following conditions and limitations:

a) Incurs minimal additional expense to Council.

b) Does not interfere with the operation of Council.

c) Is only permitted where it has a minimal impact upon email and internet resources.

d) Does not violate any Council policy or related State/Federal legislation.

e) Use may only occur during an employee's own time.

f) Privilege of use will be monitored and may be restricted or revoked at any time. Managers are responsible for monitoring usage.

g) Use does not place unnecessary or excessive burden on Council resources, e.g. large scale emailing or mass storage or transmission of electronic files.

h) Limited personal use of other ICT resources (i.e. phone, mobile phone) is generally expected to take place during the authorised user's non-work time.

i) Personal calls are only permitted on mobile phones under emergency and/or important family circumstances. Excluded Call Types are not permitted for personal use under any circumstances. For users with a valid business requirement to access excluded call types, COO authorisation is required. For all exemptions, the user's Manager is responsible for monitoring usage and ensuring suitability of use and continued business need. Managers will also be responsible for funding all costs incurred from these exemptions.

j) Usage of facilities which are provided by third parties at an expense to Council (including internet, email, mobile telephones and online applications) are subject to reporting to and monitoring by Managers, COO and the CEO to ensure fair and equitable usage and that additional contract costs are not incurred by Council. End users may have their access moderated, restricted or revoked if they are deemed to be excessively utilising services for personal use.

k) Will withstand public scrutiny and not bring an employee of the Council, a Councillor or Council into disrepute.

l) Use does not include maintaining or supporting a private business enterprise and/or use for personal gain or profit.

m) Any information created, transmitted or stored for personal purposes will not be the responsibility of the Council.

n) Information resulting from personal usage will be subject to scrutiny and/or audit at any time.

o) Any unsolicited inappropriate material from the internet or through an email is to be deleted immediately from Council systems.

Examples of Limited Use include, but are not limited to (some activities are subject to Manager approval):

a) Completing an internal job application.

b) Using the internet to access white/yellow pages online.

c) Using the internet for personal online banking. This excludes any activities relating to a private business enterprise and/or online share trading.

d) Conducting searches over the internet on appropriate and ethical topics that will not cause embarrassment or harm to the Council, during own time on authorised breaks.

e) Reading personal internet-based email is open to scrutiny and must not be inappropriate, unlawful, or criminal, and must not relate to a private business enterprise. This should be limited to authorised breaks only, during own time.

f) Printing a copy of an internet web page or email.

g) One off, local calls made from Council telephones for domestic purposes.

Unauthorised or Inappropriate Use

Unauthorised or inappropriate use of Council owned or provided ICT resources:

a) Usage which infringes copyright.

b) Involves creating, downloading, storing, viewing or distributing obscene, indecent, offensive or sexually explicit material or material unbecoming to propriety.

c) Contains untrue information that is likely to damage the reputation of a person in their profession or trade or by which other persons are likely to be induced to shun or avoid or ridicule or despise the person.

d) Downloading non-business related digital content or applications using Council provided data.

e) Contains material or images that may offend the recipient or others who may view it.

f) Bullies or harasses another person or is of a violent nature.

g) Expresses a view or commits Council to a course of action that is outside your delegated power.

h) Discriminates against a person on the basis of the person's age, race, gender, religion, marital status, sexual preferences or other unlawfully discriminatory attributes.

i) Contains internet addresses or links to material or sites that contain any of the unacceptable content cited above.

j) Any use that bypasses established and/or official channels of communication as defined by Council reporting relationships including the settlement of personal disputes.

k) Campaigning for personal gain.

l) Failing to undertake Council security procedures such as virus checking when downloading files and/or software and sharing and/or distributing network or application access passwords.

m) Any use that would interfere with the day-to-day operations of the Council and places an unnecessary or excessive burden on Council resources, e.g. large-scale emailing or mass storage or transmission of electronic files.

n) Council's call transfer service must not be used to transfer private calls in such a way that Council ends up paying for the cost of the private call.

o) Usage of and access to Excluded Call Types.

p) When allocated to a role (position) rather than to individuals, mobile phones are NOT to be used for personal calls.

q) Tampering, altering or changing any aspect of the Mobile Device Management (MDM) security software on Council supplied mobile devices and tablets.

r) Any unauthorised use that is not lawful, criminal or unethical, including usage outside permitted conditions and limitations for official, professional or limited personal purposes.

Council employees, Councillors and Contractors alleged to have inappropriately used Council ICT resources to create, download, store, view or distribute obscene, indecent, offensive or sexually explicit material or material unbecoming to propriety, e.g., pornography, will be referred to Council's CEO for investigation. This may result in the taking of disciplinary action. Any attempt to subvert existing security controls, both internal and external to Council will be noted and included in any action taken.

Examples of Unauthorised / Inappropriate Use include, but are not limited to:

a) Viewing, creating, downloading, storing or distributing materials in the workplace which are inappropriate, indecent, obscene or sexually explicit, e.g., pornography.

b) Taking inappropriate pictures with cameras or mobile phone cameras.

c) Using Council phones to call private mobile phone numbers where it is not an emergency situation.

d) Any use that incurs additional data charges to Council including but not limited to 'tethering' of data devices and using Council-supplied mobile data as a replacement for a private internet connection.

e) Forwarding inappropriate jokes, images and digital content

f) Conducting private business enterprises for personal gain or profit.

g) Downloading, storing or distributing material such as chain letters or information pertaining to pyramid schemes.

h) Creating and/or maintaining personal websites.

i) Knowingly downloading files from the Internet or storage media containing malicious code, viruses, Trojan horses, worms or Spyware that may cause harm to Council.

j) Making telephone or mobile telephone calls to subscription numbers (e.g., 1900 numbers) or overseas/IDD numbers where specific exemption has not been authorised.

k) Failing to keep Council passwords secure.

l) Expressing a view to the media outside of an authorised delegation.

m) Disrupting other ICT resources through such means as mass mailing, storage or transmission of large files or any other unnecessary activity that may place a burden on Council resources.

n) Sending unauthorised Global emails.

Unlawful and Criminal Use

Unlawful and/or criminal use of Council owned or provided ICT resources is use which violates State or Federal law and/or the *Criminal Code Act 1899*.

Unlawful and/or criminal use of Council owned or provided ICT resources by users will be subject to either criminal, official misconduct or other disciplinary proceedings against them.

Criminal and/or Unlawful Use may include

a) Publicly selling inappropriate / indecent / obscene / sexually explicit material such as pornography.

b) Exposing any inappropriate / indecent / obscene / sexually explicit material to an area where it may be publicly viewed.

c) Breaching copyright laws such as illegally copying movies, music, software programs or storing any files which you do not have explicit rights to copy, modify or store on the Council's network or using a Council supplied device or connection such as but not limited to music files.

d) Attempting to intercept, alter or steal data in order to harm Council or for personal gain.

e) Leaking confidential Council information to the media.

f) Creating or assisting in creating a computer virus.

h) Sending unsolicited commercial emails (spamming).

i) Downloading and/or storing inappropriate defamatory material.

j) Committing other offences whilst using Council ICT resources such as illegal gambling, defamation, fraud and copyright infringements.

k) Using a hand held mobile phone whilst driving.

3.4 Internet and Email

Council's corporate internet and email systems are available only for authorised users. Emails sent or held on the Council network is owned by Council and forms part of the corporate memory and must be managed and dealt with in accordance with recordkeeping and privacy principles.

There are risks and costs associated with email and internet usage, which Council seeks to minimise. There are also established corporate standards related to the way this aspect of the 'face of Council' is portrayed to the general community.

a) Authorised officers, for reasons of performance and compliance with legal obligations, will monitor general and personal usage of Council's internet and corporate email to ensure systems are appropriately used and that the system has the capacity to meet Council's business needs. Additionally, during problem resolution, authorised officers may need to view the content of email to identify causes related to performance issues.

b) Council management or its delegated officers will also regularly monitor, and audit emails stored or sent on Council's email and internet and email systems in order to ensure that authorised users are using the service in compliance with Council policy.

c) Email coded or marked as 'confidential' or 'private' by a Council source shall be treated the same as any other confidential document. However, users should be aware that system monitoring and incident management may result in some messages having to be viewed from time to time by other authorised Council staff.

User Responsibilities

All users must:

a) Comply with this policy, other relevant policies and supporting policy instruments with particular reference to the Employee and Councillor Code of Conduct.

b) Conduct correspondence in line with all delegations and authorities. These apply equally to email through usage of telephones, mobile devices, desktop, laptops and tablets.

c) Not send electronic correspondence using the identity of another person, unless authorised to act on the sender's behalf.

d) Not Send 'Chain Mail' or forward it under any circumstances using Council's corporate email system, and repetitive or disruptive incidences should be reported to management for further action.

e) Not send SPAM email or forward it under any circumstances using Council's corporate email system. Instances of SPAM should be reported to management for further action.

f) Only selected staff due to the nature of their role / duties are granted permission to send global emails. The permissions have been pre-approved by the COO or CEO and setup within Microsoft Outlook. This will prevent emails being sent to everyone globally unless generated by an authorised person.

3.5 Microsoft 365 Operating Environment

The Microsoft environment has been implemented with provision to expand the use of business applications in accordance with Council's ICT Strategy and Business Transformation Strategy.

User Responsibilities

a) Council owned end-user and peripheral devices may only be connected to the corporate network via access methods authorised by the COO

b) Network access by third parties (e.g., community groups, outsourced service delivery organisations, alliances, etc.) may only occur with the prior approval of the COO.

c) Council supports sustainable business practices. Unless there is a valid operational reason for the equipment remaining on, Council PCs, laptops/notebooks and other computing devices must be powered off at close of business to minimise power usage and to ensure daily update.

d) Council laptops/notebooks, tablets and mobile phones should be stored in a secured location, at minimum removed from public view at the end of the business day, if they remain overnight at a Council location.

e) Council laptops/notebooks, tablets and mobile phones used outside Council premises are to be kept secure.

3.6 Telephones, Mobile Phones, Scanning, Photocopy Machine

Authorised users of the Council telephone, scanning, photocopy machines and mobile phones may include employees and others engaged in activities on Council's behalf, as well as external business entities and their employees.

Council owned equipment means owned, leased, hired, or loaned equipment.

This acknowledges that there are risks and costs associated with telephone, scanning, photocopying and mobile phone usage, which Council seeks to minimise, such as loss of reputation and financial risk. They also establish corporate standards related to the way this aspect of the 'face of Council' is portrayed to the general community.

Councillors' mobile phone entitlements are described in the Council Expense Policy.

Staff Mobile Phone usage and entitlements are described in the Mobile Phone Policy and Mobile Phone Procedure

Telephone Features Requiring Approval

International Direct Dialling (IDD) and 'Voice Mail', 'Call Diversion to an external number' and Mobile Extension must be approved by the requestor's Manager.

Mobile Features Requiring Approval

IDD, mobile data services, Multimedia Message Service (MMS) and / or Global Roaming must be approved by the requesting officer's Manager.

User Responsibilities

a) All users must comply with this policy, other relevant policies and supporting policy instruments.

b) Council owned mobile telephone SIM cards must not be removed or transferred to other phones without authorisation from the COO.

c) Council owned mobile phone devices are not to be left unattended in motor vehicles unless mounted to the vehicle.

d) Users may be held personally responsible for the cost of any loss or damage of ICT equipment when such loss or damage exceeds normal wear and tear and can be attributed to negligence. All loss or damage to be reported to the COO.

3.7 Software

Copying of any software program or data sets that are subject to a licence agreement is prohibited, except for the purposes of backup or installation by Council authorised officers.

No user of licensed software or data sets may move beyond the provisions of the licensing arrangement when using these software or data sets.

No software program or data set that could be subject to a licence agreement and which exists on a device that is not owned or leased by Council may be copied to any programmable device that is owned or leased by Council, except where this is done by persons who have been authorised to carry out these tasks.

Software or data sets that relate to the configuration of any programmable device that is owned or leased by Council may only be modified or in any way changed by Council officers who have been authorised to perform these tasks. Exceptions include:

- Where the changes are authorised changes to the personalisation of the programmable device.
- Software application within the functionality of the application and accessible to the user.

Where software and data set configurations represent part of Council's Corporate Memory, those authorised to install and maintain these files must ensure that a system is in place to preserve this Corporate Information and comply with legislative standards.

The software and data set provisions of this policy are concerned with managing copyright and corruption and security risks to Council's software and data, where this software and data is operated on any Council owned or leased programmable device.

User Responsibilities

a) All users must comply with this policy, other relevant policies and supporting policy instruments.

b) No Council employee, Councillor or contractor shall knowingly breach a software licensing agreement for any software or data that is owned or leased by Council. It is the responsibility of the user concerned to ensure that no breach of licensing or copyright arrangement occurs.

c) Only authorised officers can install software that is to run on any of Council's leased or owned programmable devices.

d) Staff may be granted special authorisation as Power Users of specific applications to install executable files for their specific applications. Under no circumstances are Power Users permitted to download software from external sites.

e) Council owned or licensed software or licensed data must only be stored on a programmable device or electronic storage device that is authorised by Council.

f) Software and data can be made available on a licensed basis, for example, operating system software or on a non-licensed basis, for example, Internet cookies.

g) All data leased, licensed or owned by Council must be backed up through a means which complies with Council Policy.

h) Only an authorised person may make changes to the Operating Software or Application Software configuration. No downloads of screensavers or other programs from the Internet are permitted. No unauthorised deletions, additions or customisations may be made to the software on programmable devices that are owned or leased by Council.

3.8 Remote Access

Remote access to Council's individual staff email accounts will be available via Microsoft 365 platform. This access has the ability to be restricted at any time.

Staff utilising the BYOD mobile phone scheme will be required to download applicable applications to monitor security and perform work tasks as outlined in the Mobile Phone Procedure.

User Responsibilities

a) All users must comply with this policy, other relevant policies and supporting policy instruments.

b) All remote users are required to notify their manager immediately if they no longer require access privileges.

c) Under no circumstances will an unauthorised user be permitted to use an authorised user's end-user device and authentication key/login.

d) Council laptops should be switched off, locked or in hibernation mode when not in use, to prevent unauthorised access to the Council network and to support sustainable business practices.

4. Collaboration

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

5. Legislative Context

This Policy is not required by the *Local Government Act (2020),* however, the *Act* requires Council's to give effect to the overarching Governance principles. The policy establishes a governance framework in which staff, Councillors and contractors must adhere too.

6. References

- Mobile Phone Procedure
- Mobile Phone Policy
- Media and Communications Policy
- Information Privacy Policy
- Employee Code of Conduct
- Human Resource Policy and Guidelines Manual
- Councillor Code of Conduct
- Council Expense Policy

7. Consistency with Governance Principles Local Government Act 2020

Governance Principle	Section of policy where covered
(a) Council decisions are to be made and actions taken in accordance with the relevant law;	Section 5 – Legislative Context
(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;	Section 3 - Policy Statement and Scope
(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 4 - 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 taken into account in strategic planning and decision making;	Section 3 - Policy Statement and Scope
(i) the transparency of Council decisions, actions and information is to be ensured.	Section 3- Policy Statement and Scope

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

(b) the community engagement principles;

(c) the public transparency principles;

(d) the strategic planning principles;

(e) the financial management principles;

(f) the service performance principles.

Council Approved Policy

Policy Adopted:	Council Meeting 24 June 2020	Council Minutes Page 157
Policy Reviewed:	Council Meeting 23 August 2023	Minutes Page

YARRIAMBIACK SHIRE COUNCIL
34 Lyle Street, Warracknabeal VIC 3393
T: (03) 5398 0100
F: (03) 5398 2502

www.facebook.com/yarriambiack

PO Box 243, Warracknabeal VIC 3393
E: info@yarriambiack.vic.gov.au
W: www.yarriambiack.vic.gov.au

www.twitter.com/yarriambiackshire