GLEN EIRA CITY COUNCIL

BENTLEIGH
BENTLEIGH EAST
BRIGHTON EAST
CARNEGIE
CAULFIELD
ELSTERNWICK
GARDENVALE
GLEN HUNTLY
MCKINNON
MURRUMBEENA
ORMOND
ST KILDA EAST

# GLEN EIRA CITY COUNCIL

# Acceptable Use of Technology Policy

| | |
|---|---|
| **Date first adopted:** | March 2024 |
| **Date last amended:** | N/A |
| **Next review date:** | March 2027 |
| **Policy Owner:** | Chief Information Officer |
| **Approved by:** | Chief Executive Officer |
| **Policy Category:** | Category 4 Policy - Discretionary policy that requires CEO approval |

# CONTENTS

## 1. TITLE

Acceptable Use of Technology Policy

## 2. PURPOSE

The purpose of this policy is to prescribe acceptable use of Information Technology (IT) systems at Glen Eira City Council, in order to minimise the risk of misuse of the Council's systems and applications and ensuring the confidentiality, integrity and availability of information held by the Council. It sets out the principles required to protect Council's information assets from internal and external threats weather deliberate or accidental. This policy supplements the *24/1239 - Workplace Technology and Information Security Policy* by ensuring that all Council staff are aware of their responsibility to protect Council's information assets.

## 3. SCOPE

This policy applies to the use of information, electronic and computing devices and network resources to conduct Council business or interact with internal networks and business systems, whether owned or leased by Council, the employee or a third party.

All staff including contractors, consultants, temporary and other employees at the Council and its subsidiaries are responsible for the appropriate use of information, electronic devices and network resources in accordance with Council's policies and procedures and local laws and regulations. Exceptions to this policy are documented in *Exception* section.

The policy applies to all devices that can be connected to the Council's network, including but not limited to:

- All computer, including laptops, desktops and thin clients
- Mobile phones including smart phones
- Tablets that have been provided by the Council
- Personal portable storage devices connected to the Council's ICT resources such as USB drives and external hard disk drives and other devices that store data
- Network resources including email and Council's approved cloud and on-premises storage systems including OneDrive for Business, SharePoint, Teams and Record Management System i.e., Content Manager.

## 4. DEFINITIONS, ACRONYMS AND ABBREVIATIONS

| Term | Meaning |
|---|---|
| BYOD | Bring Your Own Device |
| Corporate Telephony Equipment | Corporate Telephony Equipment refers to telecommunication devices, such as Teams phones and other integrated hardware, designed for official business use within Council. |
| Encryption | The process of encoding information in such a way that only authorised parties can access it. |

| | |
|---|---|
| ICT | Information Communication Technology is an extensional term of IT that includes unified communications, integrations and telecommunications and computers. As well as necessary enterprise software, storage and audio-visual that enables users to access, store, transmit and manipulate information. |
| Information Security Classification | The process of categorising information assets based on their sensitivity (OFFICIAL, OFFICIAL: Sensitive or PROTECTED) and importance to Council. This helps determine the level of protection required for each asset. |
| Information Custodian | A person or party who is responsible for taking care of and protecting information asset/s at any point during their asset lifecycle. |
| Information Owner | A nominated role responsible for the secure management of all information under their control, on behalf of the owning organisation. In accordance with VPDSS an Information Owner is the person or entity that has legal possession of the information asset and are ultimately accountable for that information. |
| In Writing | In Writing is a formal document that has been sent, confirmed as received and has corresponding acknowledgement; for example, an email or letter that contains a subject, signature and date. |
| Microsoft 365 (M365) | Microsoft 365 is cloud-powered productivity platform which includes Word, Excel, PowerPoint, Outlook, OneDrive, Teams, SharePoint, etc. |
| Mobile Device | A mobile device refers to any portable electronic tool designed for personal and/or business use, such as smartphones, tablets, laptops and wearable devices, these devices are capable of communication, data storage and access to applications, typically through wireless or wired networks. |
| Must | Must is used to state mandatory requirements. |
| Network | Local Area Network (LAN), Wireless Local Area network (WLAN), Wide Area Network (WAN), Wireless Access Point (WAP), General Packet Radio Service (GPRS) |
| Official: Sensitive | This type of information is considered medium risk. If it fell into the wrong hands, it could cause limited harm or damage to government operations, organisations and/or individuals such as staff or customers. |
| Protected | This type of information is considered high risk. If it fell into the wrong hands, it could cause major harm or damage to government operations, organisations and/or individuals such as staff or customers. |
| Portable storage device | Computer data storage device that is physically removed or disconnected from the computer and must be reinserted or reconnected by a human operator before the computer can access it again. Portable storage devices include flash drive, USB keys (thumb drives), external hard drives and portable CD/DVD-ROM drives. |
| Two-Factor Authentication (2FA) | A security process that requires users to provide two different authentication factors to verify their identity. This typically involves something a user knows (like a password) and something they have (like a mobile device or security token). |
| Security Profile | The configuration settings and policies applied to a device or system to ensure its security. |
| Service/s | A service is any system that provides functionality to the Council's users and customers. |
| Sensitive information | Sensitive information means information or an opinion that relates to an individual's racial or ethnic origin or political opinions or membership of political association or religious beliefs or affiliations or philosophical beliefs or membership of a professional or trade association or membership of a trade union or sexual preferences or practices or criminal record – that is also personal information. |
| Shared Mailbox | A mailbox that multiple users can access to read and send email messages. |
| Should | Indicates a best practice action. It is not compulsory but highly advisable to follow to ensure compliance with the policy. |
| Systems | Any manipulator or holder of information that involves the input, transformation, |

| | |
|---|---|
| | storage or output of data. This may or may not include technology. Basically, Active Directory (AD), Cloud storage, database applications, document management, email, finance software and applications, Service Desk, Internet, Intranet, Operating Systems on Laptops, Smartphones and Tablet devices, Outlook, Printing, Project Management tools, SharePoint, Telephony, Building Management Systems, Closed Circuit Television (CCTV). |
| VPDSS | Victorian Protective Data Security Standard. |
| Virtual Private Network (VPN) | A secure network connection that allows users to access resources on a private network securely over a public network. |
| User/s | Means any person that must comply with the requirements of this policy. This includes, but is not limited to employees, staff, contractors, vendors, suppliers, business partners, clients and visitors. |

## 5. ACCOUNTABILITY

All personnel using the Council's information resources are responsible for knowing Council's regulations and policies that apply to the appropriate use of the Council's information technology, resources and assets. You are responsible for exercising good judgement in the use of Council's technological and information resources.

Executives and Line Managers are responsible for ensuring that all visitors, contractors and consultants have read, understood and adhere to this policy. Staff much consult their line managers if they are uncertain about any aspect of this policy. User should notify the IT Help Desk if they are aware of any breaches of this policy being committed by other persons.

## 6. POLICY

**Glen Eira City Council's Acceptable Use of Technology Policy informs all staff of their responsibilities surrounding the use of Council's information assets.**

### *6.1 General use and ownership*

6.1.1 Data created by staff on Council's systems remains the property of Council, unless otherwise agreed in writing.

6.1.2 Council proprietary information stored on electronic and computing devices whether owned or leased by Council, the employee or third party, remains the sole property of Council. Staff must ensure through legal or technical means that proprietary information is protected in accordance with the Information Security Policies and Procedures.

6.1.3 The information contained on Internet/Intranet/Extranet-related systems is classified in the *Information Asset Register*. Staff must ensure compliance with the *Information Security Classification Procedure* when gaining access to, or while handling the information.

6.1.4 Staff shall obtain explicit permission of the Information Owner and/or Custodian before sharing or allowing access to the classified information with other staff.

6.1.5 Staff have a responsibility to promptly report the theft, loss or unauthorised disclosure of Council proprietary information to the IT Help Desk.

6.1.6 Staff may access, use or share Council's proprietary information only to the extent it is authorised and necessary to fulfil assigned duties.

6.1.7 Council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. For security and network maintenance purposes, authorised individuals, vendors and/or contractors within Council may monitor equipment, systems and network traffic at any time.

6.1.8 Personal or non-business use of the systems shall only be permitted when this use does not deny the availability of network resources to other staff and does not compromise the confidentiality and integrity of Council's information assets.

6.1.9 All staff shall be responsible and liable for all actions including transactions, information retrieval or communication performed on Council's information systems following login to those systems.

6.1.10 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by Council, is prohibited and may be deleted without warning.

6.1.11 Usage should comply with all the Council policies including Council's *Staff Code of Conduct*.

6.1.12 Users of Council's ICT environment and systems must not create, send, store, access, use, solicit, publish or link to:

6.1.12.1 Offensive, obscene, profane or indecent images or material including gambling or pornography;

6.1.12.2 Material likely to cause distress or offend individuals or cultures;

6.1.12.3 Discriminating or sexually harassing material or messages that create an intimidating or hostile work environments for others;

6.1.12.4 Defamatory materials or materials that makes misrepresentations or could be otherwise construed as misleading;

6.1.12.5 Materials that infringe on the intellectual property (including copyright) of other person or organisation;

6.1.12.6 Malicious software such as viruses, worm or data harvesting software.

6.1.13 Council's ICT systems must not be used in the conduct of a personal business or unauthorised commercial activities. Limited personal commercial activities may be allowed if prior authorisation is gained from the Chief Information Officer.

6.1.14 Council's ICT systems must not be used for any illegal activity such as creating, accessing or sending chain letters, pyramid schemes, spam or attacking other computer systems.

6.1.15 Any file sharing software (i.e., BitTorrent) is not permitted.

6.1.16 Council's ICT systems are not permitted for downloading or storage of music, imagery or video content except where it deemed for the purpose of work-related activities.

6.1.17 Users must not deliberately corrupt or destroy ICT facilities.

6.1.18 Users must not install or connect unapproved hardware to Council's network

6.1.19 Council's ICT systems must not be used for cryptocurrency mining activities. The installation, operation or facilitation of any software or processes aimed at mining cryptocurrencies, including but not limited to Bitcoin, Ethereum or any other digital currency is strictly prohibited.

6.1.20 Users must not violate software licensing agreements

6.1.21 Use of Council's internet resources for personal purposes (e.g., internet banking) is undertaken at the user's own risk.

### *6.2* ***Hardware***

6.2.1 Staff are prohibited from carry out any changes to desktop configurations on workstations unless specifically authorised by the IT Help Desk.
6.2.2 Staff shall be accountable for the hardware provided to them and shall return in a good working condition at the conclusion of use of the hardware.
6.2.3 Attaching personal hardware such as external optical drives, modems and/or wireless access points to workstations is prohibited.
6.2.4 Any vendor workstation/hardware/systems must not be connected to the Council network unless approved by Chief Information Officer.
6.2.5 Staff must not physically move any workstation or hardware from the Council's premises other than laptops for assigned duties.

### *6.3* ***Software***

6.3.1 All workstations are loaded with pre-approved licensed software. Any unauthorised download and installation of non-standard software on the workstation for personal or official use is prohibited without prior authorisation or may be removed.
6.3.2 Staff are prohibited to use and distribute license keys purchased by Council for their personal use or circulation within or outside Council.
6.3.3 Staff are prohibited from making and unauthorised software configuration changes.

### *6.4* ***Physical Access***

6.4.1 Staff are responsible for the security of their systems and shall take adequate measures to restrict unauthorised physical access to their systems.
6.4.2 Third party personnel shall not access Council systems unless authorised by the relevant Business Unit Manager.
6.4.3 Theft or loss of systems or components shall be brought to the notice of the ICT Help Desk and/or reporting manager immediately.

### *6.5* ***Logical Access***

6.5.1 Access to Council systems application is for authorised staff only. Staff must not grant access to their workstation to anyone other than themselves or the IT Help Desk for support or investigation purposes without approval from their respective line manager.
6.5.2 Staff must ensure that login processes are followed when using their user IDs and passwords or any other authentication mechanism deployed by Council systems.
6.5.3 All staff must access Council's systems and applications with their own user ID and password. User ID and password must not be shared.
6.5.4 Any activity carried out under a user ID is the responsibility of the owner of the user ID.
6.5.5 All staff must ensure they lock their computer screens when they leave workstations unattended for short duration.
6.5.6 Staff shall not share files and/or folders on desktops. Use only approved applications,

such as OneDrive for Business.

6.5.7 Staff shall not have administrative access to their workstation unless approved by the Chief Information Officer for the purpose of system maintenance, troubleshooting, or other legitimate business requirements that necessitate elevated access privileges.

### *6.6* ***Password use***

6.6.1 All staff shall treat passwords as confidential information and will not share them with anyone.

6.6.2 Records (e.g., paper, software, file or hand-held devices) of passwords must not be made, unless these can be stored securely.

6.6.3 All staff shall select strong passwords (*paraphrase is highly recommended, use this online tool - https://www.useapassphrase.com*) with minimum length of sixteen (16) including alpha-numeric characters that should include uppercase characters, lowercase characters, numbers and special characters, such as $,@,*,!,etc.

6.6.4 New passwords must be different from previous used password(s).

6.6.5 Temporary or default passwords must be changed following a user's initial log-in.

6.6.6 Passwords for Council business applications must not be saved in automated log-on process, e.g., stored in a macro or function key or set to be remembered by the computer.

### *6.7* ***Email use***

6.7.1 Council allows limited personal use of the Council email that does not have an adverse impact on business operations of Council. Personal emails must not contain a Council signature.

6.7.2 Staff are encouraged to primarily use their work email accounts for sending emails. However, they may use shared mailboxes when authorised by manager or when it is necessary to conduct Council business efficiently.

6.7.3 Staff must not engage in any activity that breaches the Council's Staff Code of Conduct.

6.7.4 Forwarding of messages from Council email systems to personal accounts is prohibited unless approved by the relevant Business Unit Manager, where a valid business reason exists.

6.7.5 Staff shall not send any fraudulent or misleading offers for products and services of Council using their email account.

6.7.6 Staff shall not manipulate email for unauthorised purposes such as the use of Council-branded header or footer information.

6.7.7 Staff shall not use Council email distribution lists for non-business purposes.

6.7.8 Unexpected computer files received via external email must be deleted without being opened to minimise the risk of potential viruses spreading to their systems.

6.7.9 Personal web email accounts (such as Gmail and Hotmail etc.) are prohibited from being used for business purposes.

6.7.10 Council's corporate email account shall not be used to subscribe to any Internet news groups or websites for any purpose unless authorised by the Business Unit Manager for a valid business purpose.

6.7.11 OFFICIAL: Sensitive or PROTECTED information shall not be emailed to third parties or internal staff unless authorised by the Information Owner and/or Custodian for a

valid business purpose. If sent as an email attachment, it must be encrypted or converted into a password-protected zip file before sending to external recipients.

6.7.12 Staff with access to Council email systems through webmail accounts must access webmail accounts through secure computers. Staff should not access Council webmail from untrusted computers such as those in public and/or computers without anti-virus software.

6.7.13 Staff shall ensure that they do not download any attachments containing Council Information on computers not owned by the Council.

### *6.8 Internet use*

6.8.1 Council allows limited personal use of the Internet that does not have an adverse impact on business operations at Council.

6.8.2 Access to the Internet at Council's administrative office premises must only be enabled through authorised secure gateways. Any local connection (via modem, GPRS, WAP etc.), directly to the Internet from Council premises is strictly prohibited unless specifically endorsed by the Chief Information Officer.

6.8.3 To avoid virus infections, staff must not download active code from the Internet unless required for business purpose. For the purposes of this policy, active codes include scripts, executable software, games and utilities.

6.8.4 Staff shall not intentionally engage in any activity while using Council information systems that represents a conflict of interest with Council.

6.8.5 The publishing of Council proprietary or brand information on the Internet through blogs, news groups, collaborative or social networking sites is strictly prohibited and shall be done only by authorised business units in accordance with the Council's *Media Policy*.

6.8.6 Posting of network or server configuration information about Council, vendor, or contractor's IT infrastructure to public news groups or mailing lists and social media websites including Twitter, LinkedIn, Facebook, GitHub or other social media is strictly prohibited.

6.8.7 Any extraneous streaming of media (audio or video) such as Internet radio or television stations is not permitted, except when specifically authorised for business purposes such as viewing sessions of Parliament and/or Council Meetings.

### *6.9 Equipment and Storage Devices*

6.9.1 Users are responsible for reducing the possibility of theft, loss or damage to ICT facilities and equipment (including laptops, ICT portable devices and data storage facilities) and Council's data (stored on portable storage devices, in hard copy or otherwise) when away from the office as follows:

6.9.1.1 keep ICT facilities and Council's data secure, and preferably in their possession at all times;

6.9.1.2 if travelling by air, keep laptops with them as carry-on luggage;

6.9.1.3 do not leave laptops in an unoccupied vehicle;

6.9.1.4 immediately notify the IT Help Desk and the relevant Manager if theft, loss or damage has occurred.

6.9.2 Personal devices such as mobile phones, smart phones, tablet PCs and alike must not be attached to Council's ICT environment except to underpin business delivery.

6.9.3 It is not recommended that corporate data be stored on portable devices to minimise the impact of risk to the data.

6.9.4 The usage of cloud-based storage solutions such as Dropbox, Evernote, Google Drive and alike, to store or transmit Council's information or data is not permitted.

6.9.5 If a third party requests Council information using a non-Council approved application, ensure the information is labelled and encrypted as per the *Information Security Classification Procedure* before sharing.

6.9.6 IT Help Desk can issue Microsoft 365 for Council staff. It is the user's responsibility to ensure that Council information or data is stored securely and appropriately in the cloud-based storage.

6.9.7 Any information shall not be copied to or from portable storage devices without approval of the Information Owner and/or Custodian of that information.

6.9.8 Information classified as OFFICIAL: Sensitive or PROTECTED must be protected using encryption techniques when stored on portable storage devices.

6.9.9 Any information stored on portable storage devices must be deleted after use or prior to disposal/transfer of the storage devices.

6.9.10 Any information copied to or from portable storage devices shall be scanned for viruses before copying.

6.9.11 Laptops and Workstations are not backed up. Therefore, no Council data and/or corporate records is to be solely stored on end user devices. These documents should be stored in Council's records management systems i.e., Content Manager. Working documents can be stored in OneDrive for Business, SharePoint or Teams.

### *6.10 Fax/Print/Photocopy/Scanning Device use*

6.10.1 Staff shall ensure that unauthorised people do not gain access to printers, photocopiers, fax machines and scanners and other office devices.

6.10.2 Documents classified as OFFICIAL: Sensitive or PROTECTED must not be left unattended on any fax machine, printer, photocopier or scanner.

6.10.3 While printing/photocopying information, there should be no additional copies printed. Any additional damaged copies of printouts or photocopies should be destroyed or placed in secure destruction bins.

6.10.4 Council information shall not be transmitted to third parties without explicit authorisation from the Information Owner and/or Custodian and for valid business purpose.

6.10.5 For information being transmitted via fax, the fax number of the recipient shall be ascertained before transmission and receipt confirmation shall be obtained from the recipient on successful transmission.

6.10.6 Staff must delete scanned documents containing OFFICIAL: Sensitive or PROTECTED information from shared drive as soon as the files have been retrieved.

### *6.11 Meetings and Conversations*

6.11.1 Adequate care and caution shall be exercised by staff to ensure that OFFICIAL: Sensitive or PROTECTED information is not overheard in conversation.

6.11.2 Identity and credibility of secondary parties on telephone calls shall be established before sharing any information classified as OFFICIAL: Sensitive or PROTECTED.

6.11.3 OFFICIAL: Sensitive or PROTECTED information must not be left in telephone voicemail or answering machine messages. Intended recipients shall instead be asked in the message to make contact with the caller.
6.11.4 All parties are to be notified in advance whenever telephone conversations are being recorded.
6.11.5 Where information classified as OFFICIAL: Sensitive or PROTECTED is discussed in meetings, all attendees must be made aware of the classification of the information by the meeting chairperson or presenter, and of their responsibilities in terms of use and disclosure.
6.11.6 Information on paper, white board or on any other materials provided in a meeting is cleared/erased from the meeting room on completion of the meeting.

### *6.12 Clear Desk and Clear Screen*

6.12.1 Staff must lock their computer or log out of their system whenever it is not in use.
6.12.2 Employees are required to ensure that all information in hardcopy or electronic form is locked away at the end of the working day and when they are expected to be away from their desk for an extended period (E.g., during meetings, lunch, etc.). At the end of the working day the employee is expected to tidy their desk and to put away all office papers. Council provides secure lockers and team filing cabinets for this purpose which must be locked at the end of the day.
6.12.3 Portable computer devices such as laptops or tablets must be stored in personal lockers or can be taken offsite at the end of the work day.
6.12.4 It is recommended that portable computer devices should be shut completely down at the end of the work day.
6.12.5 Any OFFICIAL: Sensitive or Protected information must be removed from the desk and locked in a personal locker or team filing cabinet when the desk is unoccupied at the end of the work day.
6.12.6 Passwords must not be stored near a computer or written down in easily accessible locations.
6.12.7 Drafts, working papers, duplicates and reference copies that are no longer needed can be destroyed under Normal Administrative Practice by placing them in the secure destruction bin. All other documents should be stored safely as records in accordance with the *Information and Data Storage Procedure*.

### *6.13 Asset Removal*

6.13.1 IT Help Desk shall maintain a record of the IT equipment that is removed from the premises of Council.
6.13.2 Removal of any IT equipment from the Council premises shall be authorised by the relevant business unit manager prior to removal.
6.13.3 Personnel removing software or IT equipment from the Council premises shall provide proof of proper authorisation to the IT Help Desk.

### *6.14 Hybrid and Field Based Working*

6.14.1 Remote working must be approved by employee's line manager based on operational needs.

6.14.2 All IT equipment used for working away from the office shall be kept in a physically secure location at all times.
6.14.3 Staff working in public places with the Council information in physical or electronic form shall take measures to ensure that there is no disclosure of Council information.
6.14.4 Staff must use a secure Internet connection, through a Council provided Virtual Private Network (VPN) to protect data during transmission.
6.14.5 Users must not use a Personal VPN service to access Council's resources.
6.14.6 All Council data must be stored on approved cloud storage systems or secure servers, with physical copies securely stored and not left unattended.
6.14.7 Staff must use strong passwords for all systems, change them regularly and adhere to secure login processes without sharing passwords. Refer to section, *6.6 Password Use.*
6.14.8 Staff must report any security incidents promptly to IT Help Desk and their line manager.
6.14.9 IT Team shall monitor remote working compliance and Council reserves the rights to inspect files and devices to ensure adherence to *Information Security Policies and Procedures*.

### *6.15 Mobile Device Use*

6.15.1 Mobile devices shall not be used for SMS/calls competitions even where a staff has unlimited usage for SMS services or calls.
6.15.2 In case of excessive usage, staff shall provide further details if asked to verify their usage in accordance with this policy or applicable policies.
6.15.3 Staff shall take adequate precautions against physical loss or theft of mobile devices and ensure that these devices are password/PIN protected at all times.
6.15.4 Mobile devices must not be left unattended, including in luggage, hotel safe or laptop bags.
6.15.5 Mobile devices must not be lent to untrusted individuals, even for brief periods.
6.15.6 Connection of untrusted devices to mobile device, including for charging is strictly prohibited.
6.15.7 With the exception of purchases made from an approved online application store (e.g., Apple's App Store, Google's GooglePlay or Microsoft store), games, freeware, shareware, movie clips or music shall not be downloaded onto any Council mobile device unless its use is legal (does not breach copyright law) and it is specifically approved and required for work purposes. Movie clips taken with the mobile device for work purposes may be stored on the mobile device.
6.15.8 Personally owned devices may not be connected to or synchronised with the Council's systems unless approved by the IT Help Desk, and the device owner agrees to the security requirements regarding the management of the device. BYOD security requirements include:
6.15.8.1 agreement that the device will be managed by the Council;
6.15.8.2 agreement for the Council approved security profile or security settings to be applied to the device.
6.15.9 In the event of theft or loss of a staff's digital device, the staff shall immediately inform the IT Help Desk to revoke all the corporate access to the mobile device.

6.15.10 Upon leaving a job that requires a mobile device, the staff shall return the mobile device to their line manager or IT Help Desk on the last working day.

## *6.16 Mobile Device for International Travel*

6.16.1 Before travelling overseas with a Council provided mobile device, the user and/or their manager must inform the travel to IT Help Desk and is expected to confirm that the device(s) are ready for international travel.

6.16.2 While travelling, the user must stay vigilant about the surroundings and take precautions on where and how the device is used. When travelling overseas with a Council provided mobile device, user should:

- 6.16.2.1 Never leave devices or portable media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes;
- 6.16.2.2 Never store credentials with devices that they grant access to;
- 6.16.2.3 Never lend devices to untrusted people, even if briefly;
- 6.16.2.4 Never allow untrusted people to connect other devices or portable media to their devices, including for charging;
- 6.16.2.5 Never use designated charging stations, wall outlet charging ports or chargers supplied by untrusted people;
- 6.16.2.6 Avoid connecting devices to open or untrusted Wi-Fi networks;
- 6.16.2.7 Use encrypted mobile applications for communications instead of using foreign telecommunications network;
- 6.16.2.8 Never use any gifted devices, especially portable media, when travelling or upon returning from travelling.

6.16.3 Following overseas travel, user should be mindful and take appropriate precautions to ensure that the device does not pose an undue security risk to Council's network. Upon return from overseas travel, mobile devices shall be presented to the IT Help Desk for inspection to ensure no exposure or infection is present on the device.

## *6.17 Corporate Telephony Equipment use*

6.17.1 Corporate Telephony Equipment, including but not limited to Teams phones, is to be used exclusively for official business communications and activities.

6.17.2 Staff are responsible for maintaining appropriate security measures on Corporate Telephony Equipment, including password protection and any other security features provided.

6.17.3 Lost or stolen Corporate Telephony Equipment must be reported immediately to IT Help Desk.

6.17.4 Sensitive information communicated through Corporate Telephony Equipment should be handled in accordance with the Council's *Privacy Policy.*

6.17.5 Users are prohibited from making any unauthorised modifications or alternations to the configurations of Corporate Telephony Equipment. Any modifications must be approved by Digital and Technology Services department.

6.17.6 The Council reserves the right to monitor and audit the use of Corporate Telephony Equipment to ensure compliance with this policy and other associated documents.

## *6.18 Use of Artificial Intelligence (AI) Tools*

**Note**: As AI technology becomes increasingly ubiquitous in the workplace, it is important for staff to be aware of the risks and responsibilities associated with its use. AI tools such as ChatGPT, Gemini, Bing, , Grammarly, etc., can provide many benefits, such as increased efficiency and productivity, but they also pose risks related to data privacy, security and ethical use. Staff can take advantage of these tools while minimising risks to the Council and its stakeholders. Refer to Councils *Artificial Intelligence (AI) Policy* for further guidance on how AI is implemented and used within Council.

6.18.1 Staff must avoid inputting or sharing any sensitive information or proprietary information into any AI tools. This includes financial data, business plans, trade secrets, customer data, intellectual property including proprietary algorithms or large blocks of code and any other information that is not intended for public consumption.

6.18.2 Staff must not input or share any personal identifiable information (PII) into AI tools. This includes names, addresses, phone numbers, email addresses, drivers license details or any other information that could be used to identify an individual.

6.18.3 Staff should take appropriate measures to secure their devices and accounts when using AI tools, including using strong passwords, enabling two-factor authentication and avoiding using public Wi-Fi networks.

6.18.4 Staff must use AI tools in a responsible and ethical manner, avoiding any actions that could harm others or violate their privacy.

6.18.5 Any output generated by AI tools should be used in accordance with Council's policies and procedures. Staff should be cautious in using any output generated by AI tools that may contain sensitive information.

6.18.6 It is essential to note that subscription cost associated with the use of AI tools are considered personal expenses. Staff utilising AI tools must bear the responsibility for their individual subscription fees, and such cost will not be reimbursed by the Council unless deemed to be part of the approved research and development initiative.

6.18.7 Staff must use their personal email account for accessing and using AI tools. The use of Council provided email accounts for AI tools access is strictly prohibited unless deemed to be part of the approved research and development initiative.

## *6.19 Credit Card Numbers*

6.19.1 Credit Card Numbers should not be stored in files in clear text on the file server shared drives, local computer drives, or cloud-based file storage. Credit Card Numbers should not be transmitted or received via email.

## *6.20 Responsibilities of Staff*

6.20.1 Staff shall demonstrate good information security practices in their day-to-day work as prescribed in this policy and *24/1239 - Workplace Technology and Information Security Policy*. This will better safeguard the confidentiality, integrity and availability of Council's information assets.

6.20.2 Staff shall report information security incidents to their respective reporting managers and the IT Help Desk. Examples of some information security incidents are:

- 6.20.2.1 Unauthorised access;
- 6.20.2.2 Loss of Council information;
- 6.20.2.3 Unwanted disruption or denial of service;

6.20.2.4 Failure/crash of IT equipment;
6.20.2.5 Hardware resources and components lost/stolen;
6.20.2.6 Virus incidents;
6.20.2.7 Hardware, software, and operational errors that result in erroneous data;
6.20.2.8 Unauthorised use of a system for the processing or storage of information;
6.20.2.9 Changes to system hardware or software characteristics and information without the owner's knowledge, instruction or consent;
6.20.2.10 Existence of stray (unknown) user accounts.

6.20.3 Staff shall not tamper with evidence of information security incidents and/or modify or delete any audit logs maintained by the IT security system.

6.20.4 Staff shall not provide Council data to external parties unless authorised by Information Owner. Information shared externally must be handled in accordance with the *Information Security Classification Procedure*.

6.20.5 Staff are responsible for the security of their data. It is the user's responsibility to store files in a manner that is relevant to its security requirements by ensuring that only intended parties have appropriate access enabled. Staff should store important data on approved storage locations to ensure a backup is available in the event of a staff PC failure. Information must not be placed where it may be accessible to people who do not have authority to access that information. Outdated information is to be appropriately archived.

## 7. COMPLIANCE

### *7.1* ***Communication***

This Acceptable Use of Technology Policy will be circulated to all personnel. Supporting contextual policies and procedures will be communicated by line management in accordance to their applicability to Business Units.

### *7.2* ***Monitoring and Review***

This policy will be reviewed as part of an overall management review of the effectiveness of Council's information security management. A regular review process shall ensure that information security compliance is consistently observed across Council and all non-compliances are periodically reviewed.
The policy will also be reviewed in response to significant changes due to security incidents and/or changes to organisational or technical infrastructure.

### *7.3* ***Compliance Measurement***

The use of Council's ICT systems is regularly monitored by the IT Team to check for compliance of this policy. Degradation of system performance may result in detailed examination of system logs and reports to identify and resolve issues.
Council reserves the right to inspect any and all files stored in Council's ICT systems, including individual computer hard drives, email accounts and personal portable devices to ensure compliance with this policy.

Degradation of system performance caused by inappropriate use of Council's ICT systems by individuals will be referred to Manager for further action.
Non-compliance is any action or inaction that is contrary to the *Information Security Management Framework* principles, policies, guidelines and/or operating procedures.

### *7.4* ***Exceptions***

A deviation from the policy may be granted if it is clear that the costs and resources necessary for compliance far outweigh the risks of non-compliance. Any exception to the policy must be approved by the Business Unit Manager in advance.

### *7.5* ***Policy Violation***

All staff must read and adhere to the contents of this policy and all supporting security policies, procedures and guidelines.
Parties who commit a security violation shall be managed in accordance with the *Staff Code of Conduct* which may lead to disciplinary action, suspension or dismissal. Similarly, contractors, third parties and agents shall be subject to their contractual obligations.

## 8. ASSOCIATED INTERNAL DOCUMENTS

This policy should be read and applied in conjunction with the following documents:

- *23/1239 Workplace Technology and Information Security Policy*
- *Information Security Classification Procedure*
- *Artificial Intelligence (AI) Policy*
- *Information Asset Register*
- *Staff Code of Conduct*
- *Privacy Policy*
- *Media Policy*

## 9. EXTERNAL REFERENCES/RESOURCES

- *Victorian Protective Data Security Standard (VPDSS)*
- *Charter of Human Rights and Responsibilities Act 2006 (Vic)*

GLEN EIRA
CITY COUNCIL

## Glen Eira City Council

Corner Glen Eira and Hawthorn Roads, Caulfield

Mail address: PO Box 42
Caulfield South, 3162

Phone: (03) 9524 3333

mail@gleneira.vic.gov.au
www.gleneira.vic.gov.au