Council Member Information Technology Acceptable Usage Policy

Responsible Officer	Chief Executive Officer
Relevant Delegations	Director Corporate Services
Legislation and References	Local Government Act 1999

1. Devices

Council and/or privately owned devices including mobile phones, tablets, laptops and fixed computers may be used to access selected Council systems (where the risk of a cyber-security or privacy breach is considered low). The following conditions apply:

- IT assets are to be kept physically secure to the extent reasonably practicable.
- Connection of non-Council USB devices and hard disks to Council owned assets is prohibited unless approved by the Director, Corporate Services.
- Devices must automatically lock within 30 seconds.
- Devices must be protected by a secure authentication system such as fingerprint or facial recognition) or a secure password or passcode (passcodes and passwords must not be shared).
- Devices must use the latest available operating system and all supported security patches must be in place.
- Devices must be less than 6 years old or run the latest operating system if greater than 6 years.
- Laptops and personal computers must have current anti-malware protection.
- All Council records, apps, access and information must be permanently removed from the device when the device ceases to be used for Council business or when employment ceases.

2. Passwords

Access to Council emails is gained via login names and passwords.

- Passwords must not be recorded in a manner where they may be accessible to others.
- Passwords must never be emailed.

3. Internet

Personal usage of Internet access on a Council-owned asset is subject to incidental and limited usage only. Internet access on Council owned assets must not be used for:

- Accessing objectionable (including pornographic or violent) or criminal material.

- Exchanging highly confidential or sensitive information.
- Creating, storing or exchanging information in violation of copyright laws.
- Gambling, gaming, conducting a business or conducting illegal activities.
- Playing electronic or online games.
- Downloading personal items such as videos and streaming services.
- Accessing social media.

4. Email Security

Email is a major source of security risk but also an essential part of our business. Council maintains a range of controls to protect from malicious email security threats. These include Spam filtering, email security software and 'two factor authentication. Nonetheless not all malicious emails can be 'blocked', and users will be exposed to malicious emails.

Email account hacking and account impersonation are common methods for cybercriminals to send fake invoices, phishing emails, or malicious attachments. IT users must maintain awareness and vigilance in managing email security including:

- Not opening suspicious messages from external sources e.g. unexpected messages, messages from a suspicious source, email addresses that don't appear correct.
- Emails received from outside the Council's internal and secure IT environment are marked 'EXTERNAL'. This highlights that extra care is required.
- If a message seems suspicious, contact the person or business separately to check if they have sent the message. Use contact details you find through a legitimate source and not those contained in the suspicious message.
- Be especially cautious if messages are very enticing or appealing (they seem too good to be true) or threaten you to make you take a suggested action.
- If unsure, thinking carefully before clicking on links or opening attachments. Before you click a link (in an email or on social media, instant messages, other web pages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognise or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video or web page without directly clicking on the suspicious link.
- Taking care when sending emails to ensure they are addressed to the intended recipient only. Particular care must be taken when sending emails to distribution lists and maintaining privacy.
- Storage devices such as USBs or hard discs must never be plugged into mobile devices.
- Maintaining awareness and acting on advice received from Council and its IT providers in relation to email security and threats (as these are continually evolving).

5. Review & Availability

This policy will be reviewed every four years, or as required.

The public may obtain a copy for a fee fixed by Council

The policy is available on Council's website www.claregilbertvalleys.sa.gov.au

6. Document History

Approved by	Issue Date	Minute Reference – Details of Review
CGVC	15/12/2022	New Policy Adopted by Council
CGVC		