KING ISLAND COUNCIL

# Policy

## Cyber Security Policy

Responsible Officer: GOVERNANCE MANAGER

Date: 10 December 2024

Review Date: 9 December 2026

# 1. Purpose

This Cyber Security Policy outlines the King Island Council's approach to safeguarding its data and technology infrastructure. It addresses the risks associated with technology use and sets out the measures to mitigate these risks. This policy applies to all authorised users, including Councillors, employees, and contractors.

The more Council relies on technology to collect, store and manage information, the more vulnerable Council becomes to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise Council and the local community.

Council relies on information and communication technology (ICT) systems every day to conduct business efficiently, share business information legitimately between Council staff and others, and to store Council's corporate knowledge, history and records.

For this reason, Council has implemented a number of security measures, and has also prepared instructions that may help mitigate security risks. Both provisions are outlined in this policy.

# 2. Scope

This policy applies to Councillors, employees and other persons at the workplace who have permanent or temporary access to Council systems and hardware. It includes people who are authorised to have remote access to Council's systems.

This policy refers to all those covered in the scope of this policy as "authorised users".

**Roles and Responsibilities**

- **Governance Manager**: Oversees the implementation and enforcement of the Cyber Security Policy.
- **Authorised Users**: Responsible for adhering to the policy and reporting any security incidents.
- **External IT Provider**: Manages technical security measures and provides support for incident response.

# 3. Policy

**Authorised access**

Access to Council's electronic systems is available only to people with legitimate business needs and who are authorised by Council's General Manager or delegate.

Council's IT provider will only arrange or amend access for people when a request is received from a properly authorised Council delegate. If there is any doubt about the authenticity of a request, Council's IT provider will confirm the request is legitimate before proceeding.

**Confidential data**

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information, transactions or records
- Data about customers/councillors/employees
- Operating Procedures
- Records of Council's operations
- Information from Closed or Special committee meetings
- Information designated confidential by resolution of a council or special committee
- Information exchanged in email or text communications

The *Right to Information Act 2009* (Tas) and the *Personal Information Protection Act 2004* (Tas) also apply to Council. Anyone concerned about the privacy of personal information held by Council, are referred to Council's Privacy Policy.

**Protect personal and Council devices**

When authorised users use their digital devices to access Council emails, accounts or systems, they introduce security risk to our data. Councillors, employees and others who access Council's systems must keep both their personal and Council-issued computer, tablet and mobile phone secure.

Authorised users must:

- Keep all devices protected by effective passwords.
- Use an authorised antivirus product managed or approved by Council's IT provider.
- Ensure devices are not left exposed or unattended while unlocked.
- Install security updates of browsers and systems monthly or as soon as updates are available. (Council owned devices are automatically updated. Only personal devices will need to manually comply with this policy.).

- Log into Council accounts and systems through secure and private networks only.
- Not connect any devices that have been configured to use operating systems not supplied by the original manufacturer, for example Apple devices that have been "jail broken" and Android devices that have "root access" installed.

Any mobile device that accesses Council's systems, including email systems, must be enforced with a passcode lock and the ability for Council to remotely remove any of its data from the device at the Council's discretion. Typically, this action would be taken in the event of a mobile device being lost or stolen.

Additionally authorised users are not permitted to save or download any Council documents to personal devices.

Authorised users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new employees of Council receive a company-issued device, it may be automatically set up to comply with these policies.

**Keep emails safe**

Emails often host scams and malicious software (e.g. phishing scams.). To avoid a virus infection or data theft, authorised users of Council systems will:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or tell-tale give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).
- Initially open questionable attachments on an Apple device (i.e. an iPhone or iPad), as they may present little risk of infection. Due to the nature of Android open system and ability to jail-break devices it is not recommended to use Android devices for testing attachments.

Emails that may be phishing or spam should be reported by using the **Report** button in Outlook. When reporting, authorised users should select the appropriate categorisation to ensure the incident is properly logged and reviewed. This process helps improve security measures and protects the organisation from potential threats.

If an authorised user is not sure that an email received is safe, the email must be referred to Council's IT service provider.

## Manage passwords properly

Password leaks are dangerous since they can compromise Council's entire IT infrastructure. Not only should passwords be secure so they cannot be easily hacked, they should also remain secret. For this reason, Councillors, employees and others with authorised access to Council systems must:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers) and avoid information that can be easily guessed (e.g. birthdays). Good passwords don't have to be hard to remember. An example of a good password that's easy to remember is "5YellowDucks" or "Itrains9timesoutof10"; an example of a password that's hard to remember is "o4!5rGC31a".
- Avoid writing down passwords. Remember them or alternatively store passwords on a secure password management application or Council IT provided password manager.
- Keep any paper or digital document containing password information confidential and destroy it when the work is done.
- Exchange credentials only when absolutely necessary. If exchanging them in person isn't possible, authorised users should telephone instead of emailing the other person, and only exchange credentials if they personally recognise the person they are talking to.
- Change passwords whenever directed by Council's IT Provider or when there is a security risk with the current password.
- Enable Multi-Factor Authentication (MFA) on any websites or services that require login credentials, provided the website supports it. MFA adds an extra layer of protection to accounts by requiring an additional verification step beyond just a password, significantly enhancing account security.

## Transfer data securely

Transferring data introduces security risk. Authorised users must:

- Never use personal email accounts, such as Outlook or Gmail, to communicate or send files related to council business. Only council-issued email accounts should be used for all official communications and file transfers. This ensures that information is securely stored, properly monitored and complies with council data security policies.
- Avoid transferring sensitive data (e.g. customer information, employee records, council minutes) to other devices outside Council. This includes via portable storage devices, directly connected (e.g. plugged in) tablets or phones. When mass transfer of such data is needed authorised users must ask Council's IT provider for help on how to do this securely.

- Only share confidential data over secure networks. Use Council's private network, personal home internet, or a personal hotspot. Avoid using public Wi-Fi or any unsecured networks where you lack control over security. Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies to protect the data.
- Report scams, privacy breaches and hacking attempts to Council's IT provider immediately.

Council's IT service provider need to know about scams, breaches and malware so they can better protect Council's infrastructure. For this reason, authorised users must report perceived attacks, suspicious emails or phishing attempts immediately to Council's IT Provider and Governance Manager.

Council's IT provider will investigate promptly, resolve the issue and send an alert to all users when necessary. Council encourages authorised users to contact them with any questions or concerns.

**Additional measures**

To reduce the likelihood of security breaches, Councillors, employees and other authorised users must:

- Turn off their screens and lock their devices when leaving their desks for over one hour.
- Report stolen or damaged equipment as soon as possible to Governance Manager and Council's IT provider.
- Change all account passwords immediately when a device is stolen.
- Report a perceived threat or possible security weakness in Council systems.
- Not download suspicious, unauthorised or illegal software to Council equipment.
- Avoid accessing suspicious websites.

Authorised users of Council's IT systems must also comply with Council's policy addressing social media and internet usage.

Council's IT provider must install and maintain effective anti-malware software and access authentication systems and ensure all remote access is protected by a secure VPN connection.

**Protecting and preserving Council's data**

Council's IT provider will maintain appropriate back up for Council's servers and ensure that back-ups are available in the event of an interruption to the system.

In consultation with Council, Council's IT provider will prepare and maintain an effective Disaster Recovery Plan/Business Continuity Plan for its IT systems and facilities. This Plan will include:

- agreed maximum outage times and target recovery times for each element of Council's IT system.
- scheduled testing.
- provision for reports of the outcomes of testing to be sent to Council after each test.
- regular reviews of the Plan that take into account outcomes of testing, changes in systems or system risks or other changes required to reflect Council's operating environment.

Council's IT provider will provide proactive advice to Council on emerging risks to its IT environment and assist Council to mitigate these.

**RELATED DOCUMENTS**

This policy is to be read in conjunction with the following documents:

Privacy Policy
Risk Management Policy
Risk Management Framework
Social Media Policy GM Directive
Disaster Recovery Plan/Business Continuity Plan (maintained by IT Provider)

## 4. Legislation, Terminology and References

**Applicable legislation:**

All laws in connection with Cyber Security including but not limited to:

- *Right to Information Act 2009* (Tas)
- *Personal Information Protection Act 2004* (Tas)
- *Privacy Act 1988 (Commonwealth)*
- *Notifiable Data Breaches scheme*

| **Definitions** | |
|---|---|
| **Term** | **Meaning** |
| **Council** | King Island Council |

| | |
|---|---|
| **Councillor** | An elected member of Council known as a Councillor or Alderman or otherwise meeting the definition of a 'councillor' as defined under section 3 of the *Local Government Act 1993* (TAS) |
| **Employee** | A person who carries out work for Council as an employee of Council. |
| **General Manager** | The general manager of Council as appointed under section 61 of the *Local Government Act 1993* (TAS). |
| **Manager/Supervisor** | A person at the Workplace who is appointed to a position that has management/supervisory responsibilities for others or their appropriately nominated or authorised delegate. |
| **Other Persons at the Workplace** | A person, other than a Councillor, who carries out work in any capacity for Council, including work as:<br>(a) a contractor or subcontractor.<br>(b) an employee of a contractor or subcontractor.<br>(c) an employee of a labour hire company who has been assigned to work at Council.<br>(d) an apprentice or trainee.<br>(e) a student gaining work experience; or<br>(f) a volunteer. |
| **Policy** | Cyber Security Policy |
| **Workplace** | A place where work is carried out for Council. |
| **Authorised User** | A person authorised by the General Manager to access and use Councils information technology infrastructure and systems. |
| **Data Breach** | An event that causes personal information held by an organisation or agency to be lost or subjected to unauthorised access or disclosure. Examples include:<br>• a device with a customer's personal information is lost or stolen<br>• a database with personal information is hacked<br>personal information is mistakenly given to the wrong person. |
| **Encryption** | The process of converting information into a secure format to prevent unauthorized access. |
| **Malware** | Malicious software designed to harm or exploit any programmable device or network. |
| **Notifiable Data Breach** | An event under the Notifiable Data Breaches (NDB) scheme that occurs in any organisation covered by the *Privacy Act 1988* and which requires individuals and the Office of the Australian Information Commissioner (OAIC) to be notified when the event is likely to result in serious harm to an individual whose personal information is involved. |
| **Phishing** | Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity. |

**History:**

Any previous policies used by Council: Cyber Security Policy 17/09/2019 - Policy Adopted – Res No: 227/19

**POLICY VERSION AND REVISION INFORMATION**

Title: Cyber Security Policy

Policy Maintained by: Governance Manager

Policy Commencement: 10 December 2024

Policy Review: 9 December 2026

| Version No | Date | Resolution No | Responsible Officer |
|---|---|---|---|
| 1.0 | 10.12.2024 | 306/24 | Governance Manager |
| | | | |