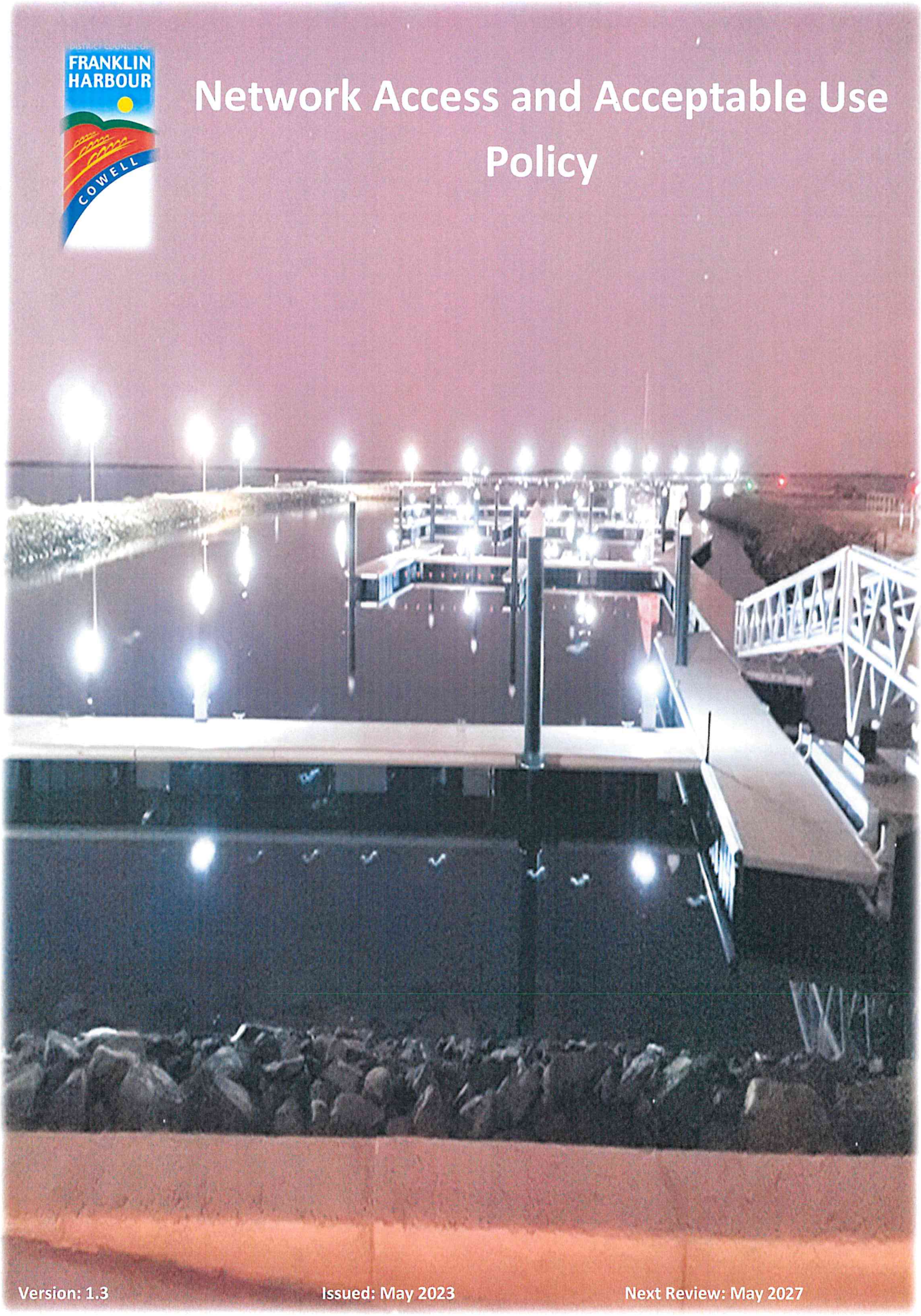
Network Access and Acceptable Use Policy



Version: 1.3 Issued: May 2023 Next Review: May 2027

Network Access and Acceptable Use Policy

Name of Council	District Council of Franklin Harbour
Responsibility	Governance
Revision Number	1.3
Effective date	May 2023
Last revised date	May 2019
Minutes reference	43/05/23
Next review date	May 2027
Applicable Legislation	District Council of Franklin Harbour Social Media Policy Local Government Act 1999, Section 109 District Council of Franklin Harbour Code of Conduct for Council Employees

1. POLICY OBJECTIVE

The purpose of this policy is to:

- Define the approach for user access to applications and systems within the District Council of Franklin Harbour.
- Ensure that the District Council of Franklin Harbour information assets are used appropriately by authorised staff, in such a way that they are an effective business tool and comply with legal requirements.
- Provide directions on the use, deployment and maintenance of mobile computing devices within the District Council of Franklin Harbour together with the remote access of such devices to the District Council of Franklin Harbour network.

2. SCOPE

The Acceptable Use policy covers all employees having access to information assets of the District Council of Franklin Harbour.

3. RISK MANAGEMENT

Risk Management is an important obligation the District Council of Franklin Harbour takes very seriously and pro-actively manages.

In the delivery of its information technology and communications services, the District Council of Franklin Harbour is very aware that there may be risks that the organisation, its employees, the Community and Stakeholders may be exposed to in relation to the security and integrity of Council's network and the information it holds.

When accessing or using Council's information technology and communications services all employees are encouraged to consider applicable perceived risks and, if necessary, communicate these to their Manager at the earliest possible opportunity.

4. POLICY STATEMENTS

4.1 Network Access & Information Security

4.1.1 Work Stations, Work Area & Physical Security

Users must have good workstation practices to ensure that unauthorised users cannot gain access to District Council of Franklin Harbour information without proper authorisation. These workstation and physical security practices are:

- Lock your PC (using a password protected screen saver) or logoff when you are away from your desk.
- Practice a clean desk policy. Make sure that all sensitive papers are put away and locked when you are not at your desk.
- Keep disks and software media secure, do not leave them lying on your desk.
- Collect printouts immediately from the printer, do not leave them lying on the printer.
- You must not post passwords or account information on monitors/desks/walls or in any other area.

4.1.2 Selection and Use of Passwords

All users shall:

- Keep their password(s) confidential.
- Avoid keeping a paper record of passwords.
- Change passwords whenever there is any indication of possible system or password compromise.
- Select quality passwords which are:
  - Easy to remember,
  - Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth;
  - Free of consecutive identical characters or all-numeric or all-alphabetical groups;
  - A mixture of upper and lower case alphabetic and numeric characters;
- Change passwords at regular intervals as forced by the system.
- Never divulge their password to another person;
- Take care that they are not being watched when typing in their password.

4.1.3 Malicious Software

Malicious software is a term used to describe programs that can maliciously attack and affect computer files and cause some unwanted actions whenever those files are used. Typically those actions include:

- Propagating the malicious software to other files on the computer system;
- Causing errors in information, for example changing values in spreadsheets or databases;
- Causing system or network overloads and thereby preventing authorised access to the systems;

- Collecting and propagating sensitive information to unauthorised third-parties (Malware or Spyware);
- Permitting unauthorised users access to the systems (Trojans);
- Allowing unauthorised access to application systems (backdoors).

As users, you should adopt the following:

- Refrain from installing browser plug-ins such as toolbar add-ins;
- Do not open any files attached to an email message from an unknown, suspicious or untrustworthy source;
- Do not open any files attached to an email message if the subject line is questionable or unexpected;
- If you need to open an untrusted attachment, always save the file to your hard drive before doing so;
- If you encounter a message on your PC screen indicating that a software virus has been detected but not cleaned you must Caramel Computing on 1300 857 450 who will act to prevent any further distribution of the virus. Do not attempt to remove virus infections yourself;

4.1.4 Incident Reporting

It is important that all suspicious events which involve the District Council of Franklin Harbour information assets are:

- Reported,
- Investigated,
- Responded to in a timely manner, and
- Evaluated for business impact.

All users have a responsibility to maintain vigilance and report any suspicious events. Such activity may include but is not limited to:

- Unusual PC activity,
- Programs behaving differently or unusually,
- Inappropriate usage of internet or email,
- If any person, at any time, asks for your password including managers, team leaders, supervisors.
- Breaches of this policy or other supporting Information Security material

You must also keep details of information security incidents confidential, and must not divulge them or discuss them with any other person, including other staff, unless authorised by the Chief Executive Officer. Any person who reports a security incident will be notified of the outcome after the incident has been dealt with and closed.

5.2 Acceptable Use

5.2.1 Acceptable Usage of Information Systems

The District Council of Franklin Harbour systems, networks, telephone, email and internet connectivity are provided for business use only.

5.2.2 Appropriate Use of Internet

All staff that access the internet through services supplied or contracted by District Council of Franklin Harbour are considered to be representatives of the business. Staff must not:

- use the internet for personal use eg accessing websites like facebook, e-bay and other such sites;
- Make any representation of the District Council of Franklin Harbour position using the internet or any other electronic means without prior consent from the CEO including, but not limited to, web page production, discussion boards, chat rooms and forums (see the DCFH Social Media Policy);
- Place the District Council of Franklin Harbour material (software, internal memos, etc.) on any publicly accessible Internet computer, except for material intended for public access on Council's official websites;
- Transmit any restricted or private information such as credit card or bank account numbers, telephone calling card numbers, log in passwords without prior management approval and reasonable security measures; and

5.2.3 Appropriate Use of E-mail

Email shall be used primarily for business purposes and shall not be used for the following:

- General solicitation (e.g. sale of products and services, with the exception of business sponsored activities, unless prior written approval is obtained from an appropriate manager);
- Charitable solicitation (requests for participation in, or financial support of, charitable activities are not permitted unless prior written approval is obtained from an appropriate manager); and
- Gambling or electronic chain letters.

Staff must not:

- Send sensitive information via email outside of the District Council of Franklin Harbour networks unless the material is encrypted using an approved technique;
- Use or access an email account assigned to another individual to send or receive messages, except through the use of delegation facilities provided and with the consent of the mailbox owner; and
- Automatically forward emails to external addresses outside the District Council of Franklin Harbour networks.

Staff shall ensure that their use of the email system does not:

- Breach a confidence;
- Defame people or products;
- Author something which constitutes misleading or deceptive conduct;

- Infringe copyrights or trademarks or breach a contract;
- Contain or transmit anything that is illegal, abusive, of a sexist, racist or offensive nature including pornographic, militant or extremist, satanic or cult, intolerant, gross depiction, violent or profane material.

5.2.4 Unacceptable Usage of Information Systems

Users must not use District Council of Franklin Harbour IT services, equipment and information for illegal, obscene, or other inappropriate activities, or in support of such activities.

"Inappropriate activity" includes any activity which:

- Interferes with the intended use of Internet resources;
- Seeks to gain or gains unauthorised access to Internet resources;
- Uses or knowingly allows another to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises, or representations;
- Without authorisation destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources;
- Without authorisation, invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources;
- Transmits, or causes to be transmitted, communication that may be construed as harassment or disparagement of others based on the criteria of any anti-discrimination legislation;
- Violates any laws pertaining to the unauthorised use of computing resources or networks;
- Violates any State, Commonwealth, Federal or International laws;
- Publishes on or over the network any information which violates or infringes upon the rights of any other person or group, including material of an abusive nature;
- Deliberately accesses, views, downloads, publishes or forwards on or over the network any offensive material including information or material that is illegal, abusive, of a sexist, racist or offensive nature including pornographic, militant or extremist, satanic or cult, intolerant, gross depiction, violent, profane or contrary to the generally accepted social standards for the use of a government facility;
- Participates in gambling activities such as may be provided by casino related sites;
- Harasses another person;
- Seeks or gains unauthorised access to any resource or entity;
- Vandalises the data of another user;
- Severely degrades or disrupts equipment or system performance;
- Misrepresents him/herself or the District Council of Franklin Harbour; or,
- Attempts to read another person's protected files without proper authority.

5.2.5 Privacy & Freedom of Information

The District Council of Franklin Harbour is mindful of the requirements of the various privacy regulations in the jurisdictions in which it operates and, in addition, that some information is generally regarded as private. However, the District Council of Franklin Harbour has the right to access, review, monitor and disclose information to:

- Ensure the information processing systems are used appropriately;
- Ensure the protection of information assets; and
- Ensure that legal responsibilities are met.

Management reserves the right to monitor, inspect and/or search at any time all of the District Council of Franklin Harbour information systems to confirm compliance with internal policies, as well as applicable laws and regulations and to monitor staff safety subject to local laws and regulations. Staff should have no presumption or expectation of privacy in their use of District Council of Franklin Harbour networks, systems and facilities.

All staff must be aware of the need to keep records and information from disclosure and that the management and its staff have a duty of care to ensure the safe keeping of all information under its control.

5.2.6 Unauthorised Software Installations

Installing unauthorised software programs on the District Council of Franklin Harbour computers is strictly prohibited. Only software approved by the Management shall be installed on the District Council of Franklin Harbour computers and networks. This includes licensed software, shareware and freeware.

All software must be used in accordance with specified license or copyright terms and conditions. Unlicensed software shall not be installed for any reason.

Copies must not be taken for use on other equipment, including privately owned equipment, unless explicitly permitted by the licensing agreement and authorised by Management.

In addition, you should observe the following:

- Certain software can be 'cracked' to bypass the authorisation or licensing requirements. Software 'cracking' is strictly prohibited and will be considered a significant breach of policy and have legal implications, even if the District Council of Franklin Harbour holds a valid software license.
- You should comply with all formal licensing requirements with regards to all software.
- You must not copy software or other material unless approved by the Management.
- You must not install or use any unauthorised software designed to compromise or bypass any security controls. Use of such software is strictly prohibited and will be considered a significant breach of policy.

5.3 Mobile Computing

5.3.1 Equipment

Mobile computing equipment is becoming a common and cost effective tool for information management and communication. The District Council of Franklin Harbour is responsible for maintaining effective security over all equipment and information within its environment.

Due to the portable nature of laptop PCs and other mobile computing equipment there is a high requirement to maintain security for any equipment maintained by the District Council of Franklin Harbour and for any information stored or transmitted via mobile computing equipment. This is particularly relevant where equipment is used outside the physical premises.

The mobile computing policies apply to the following types of devices:

- Notebooks, palmtops, tablets or laptop computer equipment.
- Mobile phones where WAP technology is used for email correspondence.
- Digital cameras or MP3 players.
- Thumb drives, diskettes, CD/DVD or other removable media.
- Other hand-held devices used for information storage and retrieval.

5.3.2 Use of Mobile Devices

The following must be observed when using mobile computing devices:

- Staff must control the amount of non business calls on mobile phones to ensure the allocation of free texts, calls and data usage on their relevant Telstra plan is not exceeded. Staff that exceed the monthly usage on their mobile phone account will be charged the excess amount for all personal calls for that month.
- Only mobile devices owned and operated by the District Council of Franklin Harbour can be used to connect to the District Council of Franklin Harbour network without prior approval from the Management.
- You must take special care to ensure that the District Council of Franklin Harbour information is not compromised through use of mobile equipment in a public place. You should attempt to ensure that screens displaying sensitive or critical information cannot be seen by unauthorised persons.
- Only District Council of Franklin Harbour equipment may be used to store District Council of Franklin Harbour data unless prior approval by Management.
- You must never leave laptop PCs or other mobile computer equipment unattended in a public place, or in an unlocked house or office. Where possible, they should be physically locked away, or special locks should be used to secure the equipment.
- Where possible, you must never leave laptop PCs or other mobile computer equipment in a car. If equipment needs to left in car for brief periods, it must be placed out of sight in the boot and the car securely locked.
- When travelling by plane, you should carry the laptop PCs or other mobile computer equipment as hand luggage.
- You must not remove anti-virus software, and make sure the anti-virus software is up to date.
- Any critical information that has been generated and stored on a mobile device should be backed up to an appropriate network location as soon as possible.
- You must not store sensitive information on a mobile device, unless it is encrypted.
- Do not attach or connect mobile devices (i.e. USB thumb drives) of unknown origin to District Council of Franklin Harbour equipment.

6. DOCUMENTATION

Local Government Act 1999, Section 109
District Council of Franklin Harbour Code of Conduct for Council Employees

7. FURTHER INFORMATION

Members of the public may inspect this Debt Management Policy at the principal office of the District Council of Franklin Harbour, 6 Main Street Cowell SA 5602, and on payment of a fee obtain a copy. A copy may also be downloaded from the Council website www.franklinharbour.sa.gov.au.

8. REVIEW OF THE POLICY

This Network Access and Acceptable Use Policy will be reviewed by the District Council of Franklin Harbour within 12 months after each general election of Council. However, Council has the right to review this Policy at any time, if considered desirable.

SIGNED: .....

Acting Chief Executive Officer

Date: 12 / 5 / 2023

User Declaration

I have read and understand the Network Access & Acceptable Use Policy and I will observe and be bound by the conditions of the Policy at all times.

Surname..... Given Name.....

User Signature..... Date.....

Change History

Version	Issue Date	Change
1.1	June 2016	New Policy
1.2	May 2019	Reviewed and Updated (post election)
1.3	June 2023	Reviewed and Updated (post election)