Information Technology Policy

CONTROL:

Policy Type:	Administrative
Authorised by:	Council
Head of Power:	Not Applicable
Responsible Officer:	Chief Executive Officer
Adopted / Approved:	Minute No. 2021.11.15-OM-6
Last Reviewed:	October 2021
Review:	October 2023
Version:	2

1. INTRODUCTION

1.1 PURPOSE:

This policy seeks to provide guidance regarding the appropriate use of information technology equipment and software while performing duties for Council. This includes all Council provided and privately owned equipment and software. IT hardware includes all personal computer and communication devices such as laptops, tablets, desktops, mobile phones, satellite phones, fixed line phones, printers, fax machines, copiers etc. IT software includes all desktop applications, web-based applications, mobile phone apps etc.

1.2 POLICY OBJECTIVES:

To establish a set of standard conditions to ensure obligations when using information technology in the workplace are understood. Council aims to provide relevant, useful and up-to-date equipment and software to assist employees in the effective and efficient performance of their duties.

1.3 COMMENCEMENT OF POLICY:

This Policy will commence on adoption. It replaces all other Information Technology policies of Council (whether written or not).

2. POLICY

2.1 CONTEXT:

This Policy applies to all Council employees, and where applicable to Contractors and Councillors as well. This Policy does not form part of any employee’s contract of employment.

2.2 POLICY STATEMENT:

The aim of this policy is to provide some legal, ethical and operational guidelines as to what constitutes best usage of Councils equipment and software.

3. STANDARDS AND PROCEDURES

3.1 SPECIFIC AND STANDARD

3.1.1 ICT Steering Committee

An ICT Steering Committee will be established and maintained. The main purposes of the committee are to:

- ensure a coordinated, whole-of-organisational approach is applied for ICT.
- identify, manage, mitigate and review ICT risks in the strategic, operational, and project risk registers

3.1.2 Service Requests

A system for employees to submit service requests to the IT Administrator will be established and maintained. The IT Administrator will regularly provide reports to the ICT Steering Committee.

3.1.3 Eligibility for a Mobile Phone

- An employee may be eligible to have a mobile phone if, in the view of the CEO it is deemed necessary for the appropriate performance of their position. For example, if the employee's duties require them to spend time out of the office and/or to be contactable outside the normal hours of work.
- A mobile phone request form must be completed and authorised by the supervisor, Manager and CEO.
- All employees issued with mobile phones must sign an agreement that defines the conditions of use.
- Where unique circumstance exist and with the agreement of the Chief Executive Officer, an employee may use his or her own mobile phone for work-related purposes according to the terms agreed with the CEO.

3.1.4 Eligibility for a Laptop

- For the purposes of this policy the term laptop encompasses all mobile computers including laptops, notebooks, tablets etc.
- An employee may be eligible to have a laptop if, in the view of the CEO it is deemed necessary for the appropriate performance of their position. For example, if the employees duties require them to be mobile within the office or perform work outside the office or at home.
- A laptop request form must be completed and authorised by the supervisor, Manager and CEO.
- All relevant employees not eligible for a laptop will be issued with a desk top computer.

3.1.5 Eligibility for Printers and Multifunction Machines

- An employee may be eligible to have a printer or multifunction machine in their office if, in the view of the CEO it is deemed necessary for the appropriate performance of their position. For example, if the employee's duties require them to regularly print or to print confidential material.

- Where colour printers are provided the default setting will be black and white. The colour setting should only be used when necessary.
- Where double sided printing is available the default setting will be double sided.

3.1.6 Camps

- Camps will be allocated with equipment as required and authorised by the CEO.

3.1.7 Equipment Purchase, Repair and Replacement

- The Systems Administrator will be responsible for arranging all repairs to equipment and purchase of replacement or new equipment in accordance with the replacement schedule.

Equipment	Replacement Schedule
Desktop Computer	Minimum 3 Years
Laptop Computer	Minimum 3 Years
Servers	Minimum 5 Years
Printers	Only when no longer operational
Mobile Phone	Only when no longer operational or out of contract
Fixed Line Phone	Only when no longer operational
Satellite Phone	Only when no longer operational

- Equipment will be recycled through Council to maximise it’s life.
- The CEO is responsible for authorising all requisitions for equipment repair and purchase in accordance with this policy.

3.1.8 Return of Council Provided Equipment

- On termination of employment or otherwise at the request of Council, an employee who has been issued with any Council provided equipment must return the equipment to their Supervisor. Any battery chargers or other accessories supplied by Council must also be returned.
- On termination of employment or otherwise at the request of Council, software login accounts and website access will be transferred, closed or cancelled.
- Employees must leave all work related files on the equipment, that is, do not delete files before returning the equipment.
- Final pay may be withheld or delayed pending return of equipment with all work related files intact.

3.1.9 Equipment Security and Care

- In accordance with Council's Code of Conduct clause 4.8.1 Using Council Assets, the employee designated as the holder of the equipment is responsible for ensuring the equipment is:
    - Cared for, kept clean and good working order;
    - Secured to protect against damage, theft and misuse.
    - Not used for any illegal purpose.
- Equipment must be password or pin protected when unattended for extended periods of time.
- Employees issued with mobile phones must set up an Apple ID using their Council email address and enable "Find my IPhone". This will provide a higher level of security, preventing the phone from being wiped.
- Equipment should normally be stored overnight or during periods of leave in a Council office, or depot. Where an employee has been granted Private or Take Home privileges on their Information Technology Equipment Agreement, the employee must secure the equipment as if it were a personal possession.
- Care should be taken when consuming food or drink near equipment.
- No stickers or magnetic items are to be placed on equipment.
- If Council believes an employee is using equipment irresponsibly, unreasonably, or in breach of this policy then the employee may have the equipment removed.

3.1.10 Lost, stolen or damaged

- If equipment is lost, stolen or damaged, it should be reported to the System Administrator and Supervisor as soon as that event occurs and an Incident form completed.
- Stolen phones should be reported to the System Administrator immediately so that they can be locked down to prevent unauthorised use.
- Faulty equipment should be reported to the System Administrator promptly.
- Depending on the circumstances, the employee may be held responsible for replacing the equipment if the loss, damage or theft was caused or contributed to by the employee's lack of care.

3.1.11 Private Use of Council Provided Equipment

- Council provided equipment is predominantly for work related use. In accordance with Councils Code of Conduct clause 4.8.1 Using Council Assets limited personal use of Council provided equipment is allowed. Limited personal use means use that is infrequent and brief, and is performed during non-paid time, that is, before and after work or during meal breaks. Refer to the definition of Limited Personal Use for more information on what is allowed and what is not allowed.
- In accordance with Councils Code of Conduct clause 4.8.1 Using Council Assets, you must not store any personal files on Council provided equipment in excess of 20% of the storage capacity of the device. Where storage capacity on the device is consumed, private files must be deleted to allow the device to continue to be used for work purposes.
- Where an employee is found to be using Council provided equipment for excessive private use the equipment may be removed or their use closely monitored until a more

limited personal use is achieved. In circumstances where a financial cost can be calculated eg use of a phone, the employee may be requested to reimburse Council. Excessive private use is defined as spending more than half an hour per day, or costing more than $5/week, or storing more than 20% of the storage capacity of the device of private data.

- The Executive Management Team (CEO, DCEO and Infrastructure Manager and Community Sustainability Manager) are eligible for private use of telephones as part of their conditions of employment. This recognises the on call nature of the role and that the employee will undertake work whilst at home.

3.1.12 Use of Mobile Phones (including Satellite phones)

3.1.3.1 Council Provided Mobile Phones

- Council supplied mobile phones are to remain on and audible during working hours except where in a meeting.
- Council officers (including Executive Management Team) with emergency contact or on-call roles such as the Town Supervisors will keep their Council supplied mobile phone on at all times.
- Photographs or videos of Council or Department of Transport and Main Roads funded work sites or camps taken on a council mobile phone must not be uploaded to social media without the approval of the CEO.
- Where Council mobile phones are provided, it is expected that the employees work email account is accessible via the smart phone and that the employee regularly checks work emails during working hours.
- Where private email accounts are accessed through the work smart phone, the employee should ensure that private emails are sent via the private email account otherwise they will be subject to the content of this policy.
- Accessing private emails and social media during work hours is prohibited.

3.1.3.2 Private Mobile Phones or Communication devices (eg Apple Watches) in the Workplace

- Private mobile phones must be on silent at all times and may only be answered in cases of emergency or during designated work breaks.
- No photographs or videos of Council or Department of Transport and Main Roads funded work sites or camps are to be taken on private phones.
- The use of social media during work hours is prohibited.
- Private mobile phones brought to work by an employee are done so at the employees risk. Council will not be responsible for the loss or damage to any private mobile phone which occurs on a council work site or during work hours.

3.1.3.3 Council Provided Mobile Phone in the Vehicle/Plant

- Employees must not use a mobile phone while operating a vehicle/plant unless a ‘Hands-free Car Kit’ is installed. Employees must obey the Queensland road rules.

3.1.3.4 Mobile Phones in Meetings

- It is common courtesy to switch mobile phones off before entering a meeting.
- Council understands that extenuating circumstances may exist that require employees to leave the mobile phone switched on during meetings. If this is the case, then employees should politely inform the other attendees prior to the commencement of the meeting that they may be expecting a call and so their mobile phone will be left on during the meeting.

3.1.3.5 Mobile Phones and Safety

- The use of mobile phones in certain parts of the workplace and in vehicles can create unsafe situations or potentially unsafe situations.
- Supervisors and managers may issue general notices or particular notices to employees and contractors regarding the use of mobile phones if they perceive a real or potential occupational health and safety risk.
- Employees and contractors are required to comply with such orders, directions and notices issued by supervisors or managers.

3.1.13 Voice Mail and Call Diversion

- An Employee must activate the voicemail set up on their phones (fixed and mobile) so that calls divert to voicemail when unanswered or busy. Messages should be dealt with in a timely manner. Employees should ensure they clear their voicemail regularly.
- Council Fixed-line phones will allow up to three recorded voicemail greetings to be recorded. Employees should set up two voicemail messages as follows.
- The standard voicemail message should say “Hello, this is (name), (position title) of Diamantina Shire Council I am unable to take your call right now so please leave your name, number and a short message and I will return your call shortly”. As mobile phones only allow one message this should be modified if an employee is on leave.
- The ‘on leave’ voicemail message should say “Hello, this is (name), (position title) of Diamantina Shire Council I am on leave until [date]. If the matter is urgent please ([ring my mobile on ##] or [ring reception and ask for [appropriate person]) otherwise please leave your name, number and a short message and I will return your call when I return from leave”.
- If an employee has a Council provided mobile phone and they will be out of the office for work-related purposes for more than 1 hour, the employee should divert calls coming in via their fixed telephone to their Council mobile phone.

3.1.14 Software Security

- Windows login passwords will be scheduled to change at least every 45 days.
- CEO must authorise all security and access settings for Council’s corporate information systems such as Synergy Soft and Infoxpert.
- Employees and contractors will be responsible for the keeping their software and website access passwords secure and protected against unauthorised use.
- Employees and contractors will not reveal their passwords to anyone including other Council employees via any means.
- Employees and contractors must report security breaches to the Systems Administrator and their Supervisor immediately.

3.1.15 Virus and Spyware

- The Systems Administrator will maintain virus scanning and spyware detection software to reduce the risk of viruses and spyware infecting Council's systems.
- Employees, Contractors and Councillors must remain alert to possible virus and spyware infections and alert the Systems Administrator immediately of anything suspicious.
- Removable USB storage devices are strictly prohibited.
- Other removable storage devices such as camera storage must not be plugged into any private equipment.
- Employees, Contractors and Councillors must immediately remove the network lead and/or turn off their equipment immediately if they have any suspicion of a virus.
- Employees to undertake regular cybersecurity training to raise awareness of virus's etc.

3.1.16 Software Purchase and Installation

- The Systems Administrator is responsible for the purchase, installation and configuration of all software including mobile phone apps.
- Removal or transfer of any council software to privately owned equipment is prohibited.
- The CEO is responsible for authorising all purchase requisitions for software or licences.
- Employees, Contractors and Councillors will consult the Systems Administrator regarding any additional software requirements. Employees, Contractors and Councillors are strictly prohibited from purchasing and installing any software including mobile phone apps without the express permission of the Systems Administrator.
- Employees, Contractors and Councillors will not modify the configuration of software except for security, accessibility or efficiency reasons.
- Employees, Contractors and Councillors will report any software problems to the Systems Administrator as soon as possible.

3.1.17 Internet Access and Usage

- Employees, Contractors and Councillors are encouraged to use the internet for work related research and investigations. The internet is an excellent tool for researching new technologies and sourcing materials and services.
- Employees, Contractors and Councillors are not permitted to:
    - Access sites that contain sexually explicit or offensive material. If an employees accidently connects to such a site they must immediately disconnect and inform the Systems Administrator;
    - Access or use any social media applications;
    - Perform malicious activities, spread virus's or use malicious programs that overload or disable any computer system or network;
    - Download and install any software, including free software, without the express permission of the Systems Administrator.

3.1.18 Electronic Mail

- Each employee and councillor will be provided with an external email account using the naming convention of [first name].[surname]@diamantina.qld.gov.au which must be used for all general related business.
- The Systems Administrator will create the signature for each account based on the Council signature format template. Changes to the layout, font or colour is in breach of this policy.
- Employees, Contractors and Councillors should remain alert to potential spam emails and notify the Systems Administrator of any suspicious emails before opening. Better to be safe than sorry.
- Council is aware that non work related emails do circulate. This policy does not seek to completely suppress such behaviour, however employees, contractors, and councillors must maintain due care in that these emails are not of an offensive nature and that fellow employees are respected.
- Emails are not permitted to be sent with large files as attachments. Attachments should be no more than 30Mb in size to ensure recipients on low speed connections do not have their systems overloaded.
- Employees are responsible for ensuring emails that constitute a Council record are registered in Council's EDRMS.
- Employees, Contractors and Councillors are not to send private emails from the Council email account.

3.1.19 Data Storage

- Council has an Electronic Document and Records Management System (EDRMS) to store all council documents and records. The EDRMS is backed up daily.
- Council provides a shared network storage area (H: Drive) which is backed up daily. This area should only be used for large files such as photos and videos
- Council provides a private network storage area for each employee with a system login account which is backed up daily. Employees are responsible for periodically cleaning up this area and ensuring all Council records are transferred to Council's EDRMS.
- All Council records and important data must be stored on Council's EDRMS or network.
- Employees must not store Council records or data on local PC hard drives or other external storage devices as these are not backed up.

3.1.20 Monitoring and Inspection

- Council reserves the right to inspect and/or monitor equipment usage including all files stored on the equipment or on the Council network or removable media to ensure compliance with this policy.
- Council may use software to identify inappropriate or sexually explicit internet sites.
- Council reserves the right to block access to certain internet sites and resources.

3.1.21 Records

- Employees issued with a mobile phone or laptop will sign an Information Technology Equipment Agreement and comply with all conditions of this policy.

- The Systems Administration will maintain a register of all Council issued mobile phones and Information Technology Equipment Agreements.
- The Systems Administrator will maintain a register of all information technology equipment. PDQ Inventory scans the network for all connected devices and identifies the software installed on the equipment.
- The Systems Administrator will maintain a register of all website access accounts. Employees, Contractors and Councillors must send the Systems Administrator the details of all website access accounts including website address and administrator details. The Systems Administrator must be notified when administrator details change.
- The Systems Administrator will maintain a register of all paid mobile phone apps.

3.1.22 Breaches of this Policy

- All employees are responsible for reporting any use of software or equipment in breach of this policy to the relevant manager for investigation.
- Breaches of this policy may lead to disciplinary action.

4. REFERENCE AND SUPPORTING INFORMATION

4.1 DEFINITIONS:

To assist in interpretation, the following definitions shall apply:

Word / Term	Definition
Council	means Diamantina Shire Council.
Limited personal use	Use that is infrequent and brief and is performed during the employee's non-paid time. That is, before and after work or during meal breaks. • Personal use is activity conducted for purposes other than undertaking official business, professional duties, and/or professional development. • Examples of permitted limited personal use include: (a) internet access that is incidental to employment or personal business transactions such as accessing government information sites and online banking and bill paying; (b) participation in approved online training or personal development programs; (c) sending or receiving infrequent personal messages by email, providing the content of the message does not breach Council's Code of Conduct or Corporate Policies. • Examples of limited personal use that is NOT permitted (not an exhaustive list) include: (a) gambling (including gaming, online betting, bookmaker odds, lottery pages, bingo, football tipping); (b) games (including traditional board games, card games and role playing games, for example, Solitaire and World of Warcraft); (c) participation in online auctions (including eBay); (d) dating (including the use of online dating services);

	(e) downloading and storage of music, video files and pictures (including the use of YouTube, iTunes, Napster, BitTorrent and similar sites/programs); (f) accessing social networking sites (including Facebook, Twitter, MySpace and similar sites) unless the use is directly connected with your duties, is for the purpose of communicating approved Council publications and/or media releases and has been approved by your team leader/ supervisor/ manager; (g) accessing, downloading, storing or sending racially and//or sexually offensive, obscene and/or other threatening, belligerent or libellous electronic communications.

4.2 RELATED POLICIES, LEGISLATION AND DOCUMENTS:

Links to supporting documentation
Code of Conduct
Corporate Communications Policy
DSC Template - Information Technology Agreement
ICT Steering Committee – Terms of Reference (Doc ID 161916)
Information Technology Equipment Register
Telstra Local Buy Contract
Website Access Accounts Register

4.3 VERSION CONTROL:

Previous Version Number	**Adopted/Approved Date**
1 (Original)	December 12 2018;Minute No. 2018.12.17-OM-12