Gladstone Regional Council

Corporate Standard

Title	**INFORMATION, COMMUNICATIONS AND TECHNOLOGY**
Corporate Standard No.	**CS-2019-12**
Business Unit/s	**STRATEGY AND TRANSFORMATION**
Date of Approval by CEO	
Date of Effect	
Review Date	
Date Repealed	

1.0 PURPOSE:

This corporate standard sets out the terms and conditions for acceptable use of our Information, Communications and Technology (ICT) resources in support of the business's corporate objectives.

2.0 SCOPE:

This corporate standard applies to all users of the business's ICT resources.

3.0 RELATED LEGISLATION:

- *Local Government Act 2009*
- *Local Government Regulation 2012*
- *SPAM Act 2003 (Commonwealth)*
- *Information Privacy Act 2009 (Queensland)*

4.0 RELATED DOCUMENTS:

- Code of Conduct Policy
- Councillor Code of Conduct Policy
- Information, Communications and Technology Policy
- Records Management Policy
- New Users Form
- Information, Communications and Technology Strategic Plan
- ICT Choose Your Own Device Catalogue

5.0 DEFINITIONS:

To assist in interpretation of this corporate standard the following definitions apply:

"Application Software" means the Standard Operating Environment (SOE) and any specialised applications approved by the Manager Strategic Information, Communications and Technology.

"CYOD" *(Choose your Own Device)* means approved users with access to the business's data and systems are given a choice regarding the device provided by the business that they will be using.

"Electronic communication" means any form of electronic mail sent from one user to another through the network or the internet, including but not limited to emails text messages, Skype IM, attachments, faxes, voicemail, and any other internet-based messaging systems.

"Employee" means a person employed directly by the business, either under an Employee Employment Agreement or the Certified Agreement.

"Executable File" means any file, program, and group of files or compressed files capable of independent execution. Including, but not limited to files with extensions exe, msi, bat, com, vbs, vbe, scr, hta, sct, shs, pif, etc.

ICT resources means all of the business's information and communication technology resources and systems including, but not limited to, telephones, mobile phones, voice mail, SMS, facsimile machines, email, the intranet, computers, printers, scanners, or any device connected to the business's network, or use of any part of our network to access other networks.

"Leader" means the Executive Team, Managers, Team Leaders and any other supervisory position that reports to a General Manager (i.e. Specialists) of the business.

"MDM" *(Mobile Device Management)* means the system used to manage email and corporate system access for mobile devices like smartphones, tablets and others. All devices enrolled in the MDM system are subject to the policies configured and enforced through that system.

"Mobile Device" means a portable device that can be used on the network and off the network with the dual boot image.

"Removable Media" means any removable disk, external hard drive or compact disc capable of transferring files or data from one computer to another.

"*Remote Access*" means any form of access to the business's network via VDI.

"Remote User" means all users who access the business's ICT resources via the internet.

User means any employee, volunteer, contractor, consultant, auditor or any other user, internal or external, with access to the business's ICT resources.

"Virtual Desktop Infrastructure (VDI)" means a remote access platform giving staff access to a virtual Windows 10 computer with all software and services available from a remote location (from their home computer or from a remote business site/office).

6.0 STANDARD STATEMENT:

The following terms and conditions for acceptable use of the business's corporate information, communications and technology resources must be observed at all times.

6.1 Network Access

All users must have a valid user account to access ICT resources, except those employees who are able to access the required ICT resources through the business Kiosks.

The business allows three types of network access:

1. network connection through the business's Choose Your Own Device arrangement (work assigned desktops, tablets, mobiles);
2. remote access via personal computers through virtual desktop infrastructure (VDI) access technology; and
3. remote access via business computers, available at the business's kiosks.

6.1.1 Creating an account

The ICT team will create a new account following written permission from the user's leader; once the leader has provided all the information necessary to build the new user profile.

6.1.2 Passwords

- Users shall not disclose their network login password, their application software login passwords, or those of any other person except if required by the ICT team;
- Remote users may provide their passwords to the ICT team for support purposes only, if requested to do so, to avoid excessive password changes;
- User login passwords should meet the password complexity requirements:
  - Minimum of 8 characters;
  - Contain a number and a special character (i.e. a symbol or capital); and
  - Must not be a password previously used;
- Passwords must be changed whenever:
  - ICT resources automatically prompt the user to do so;
  - in the absence of the user, an ICT team member with the appropriate level of access has needed to use the user's profile and has reset their password to do so;
  - a user suspects their password has been compromised; or
  - a user is requested to do so by the ICT Team.

6.1.3 Access to Another User Account

Only the Chief Executive Officer (CEO) may authorise access to examine another user's ICT communication accounts (including electronic communication records, browser history, and personal drives) for operational, maintenance, compliance, auditing, security or investigative purposes. Members of the ICT team are exempt from requiring authorisation when performing their normal operational duties.

6.2 Choose Your Own Device (CYOD)

Leaders can elect the device of their preference for their team from the ICT Choose Your Own Device Catalogue. The business will not permit access to the network through personal devices, except where remote access has been approved. Remote access is only available via personal computer not other personal devices such as tablets or mobiles.

6.2.1 Protocol

Any requests for laptops or mobiles supplied as part of CYOD for the purpose of remote access must be submitted by the user's leader to the ICT Service Desk for consideration. Requests are subject to budget availability.

6.2.2 Replacement

Tablets and smart phones will be replaced after a minimum of 3 years.

Desktop computers and laptops will be replaced after a minimum of 5 years.

Devices damaged prior to the replacement schedule will be repaired in the first instance. Where a repair is not possible, a device may be replaced outside of the replacement schedule.

A device may also be replaced outside of the replacement schedule with the approval of a Leader.

6.3 Websites

The business's public websites and intranets are both managed by the Digital Communications Advisor. For assistance or training with the website contact webmaster@gladstone.qld.gov.au.

All other websites are managed by their respective business's areas. For technical support contact the websites' host.

6.4 Geographic Information System (GIS)

The business's GIS is the primary source for spatial information. The Insights and Innovations team is responsible for its management. Accuracy of information linked from other systems remains the responsibility of the administrators of those systems.

6.5 Training

- Users will be given an ICT summary document for acknowledgement of responsibilities at employee induction training;
- For GIS training users' leaders must contact the GIS team directly to discuss training needs;
- For training for the website contact webmaster@gladstone.qld.gov.au.

6.6 Responsibilities

Users, leaders and ICT responsibilities are outlined in Attachment A.

7.0 ATTACHMENTS:

Attachment A - ICT Users, Leaders and ICT Team responsibilities.

8.0 REVIEW TRIGGER:

This corporate standard will be reviewed when any of the following occur:

1. The related legislation or governing documents are amended or replaced; or
2. Other circumstances as determined by resolution of Council or the CEO; or
3. Three years from date of effect.

TABLE OF AMENDMENTS		
Document History	**Date**	**Notes (including the prior CS No, precise of change/s, etc)**
Originally Approved	16.12.2014	CS-16/2014 Computer and Telecommunications Corporate Standard
Amendment 1		
Amendment 2		
Amendment 3		

APPROVED:

....
LEISA DOWLING
CHIEF EXECUTIVE OFFICER

Attachment A – Users, Leaders and ICT Team responsibilities

Responsible person/ Business Unit	Responsibilities per Area	Responsibilities per Area
Users	**Security, Software and Foreign Devices**	**Users of Remote Access**
	Comply with all applicable laws, regulations, policies, and corporate standards, including the Code of Conduct, while performing their duties for the business.	Provide written permission from their leader to gain remote access to corporate systems prior to actioning it with the ICT team, as appropriate.
	Register electronic information which relates to the business in the records management systems. Remember the permanent storage of information is in the records management system rather than email boxes.	Make every reasonable attempt to secure their remote device against unauthorised access including keeping anti-virus software up to date.
	Request the purchase of removable media through the appropriate business unit budget.	Log off or 'lock' a remote session when unattended or no longer required.
	If additional software is not available on the software centre, contact the ICT service desk to request installation on the business's desktop computers or laptop devices (including GIS software).	Only use remote access of the business's corporate system via communications systems which require a password upon log in. Open access networks (e.g. airport network) should not be used for the business's remote access.
	Shut down and turn off desktop computers unless otherwise requested to do so by the ICT team when leaving buildings for extended periods.	Report lost, stolen or damaged devices to the ICT team as soon as the user is aware of the event and log the incident on the business's incident management system.
	Log off or 'lock' workstations before moving away from the device.	**Users of CYOD**
	Only access the business network for limited personal use if it does not interfere with performing duties or impacts on the operation of our ICT system.	Be aware that registration through the Mobile Device Management (MDM) system will allow the device to be monitored and controlled through corporate policies that can have an impact on privacy and functionality.
	Keep Council data and information secure. Users will respect software settings designed to improve security and protect the network and desktop computer from malicious attack by not interfering, disabling or enabling settings.	A private SIM card is unable to be used in a business owned device and a business SIM card is unable to be used in a privately-owned device.
	Commit to acting ethically by not knowingly obtaining unauthorised access to information (including passwords, accessing shared mailboxes when not a member of that team, and logging onto ICT resources on behalf of another user, unless otherwise approved by the ICT Team).	Users are accountable for any loss, damage or theft to any CYOD assigned to the user.
	Preserve information. Information should not be damaged, deleted, inserted or otherwise altered with malicious intent.	Report any CYOD incident on the business's incident management system.
		Information Communication Technology
	The business's electronic communication system is to be used for the distribution of information that is legitimate business. Joke emails, SPAM, hoax emails, chain mail and advertisements are not legitimate business.	Keep personal phone calls and similar telecommunication uses to a minimum and must not make private international phone calls through the business's telecommunication facilities.
	The business's ICT resources are not to be used to conduct private business, gamble, download, distribute or use pornographic material.	Must return the business's mobile devices to the ICT Team, upon cessation of employment with the business.
	Consider the security of internal networked desktop computers and laptops. Devices should not be installed or configured to any internal networked desktop computer or laptop.	Users granted with the business's mobile devices are not the device owners.
	Only store business data on the business network.	Report any faults or queries to the ICT team as soon as possible.
		Applications, Back-ups Data Storage and Schedule Maintenance
		The network drive data for Users logged on after business hours will not be backed up on that day.
		Remote users may be denied access during maintenance periods.
Leaders	**Remote Access**	**Information Communication Technology**
	Communicate any changes on staff remote access permissions to the ICT Team.	Submit requests for telecommunication devices, fixed lines and data lines to ICT.
		Complete a New Users Form for any contractor that requires network access and submit to the ICT Service Desk. All forms must have an expected end date.
		Select the most appropriate device from the CYOD Catalogue for staff based on their work profile/location.
ICT Team	**Security, Software and Foreign Devices**	**CYOD**
	Use web and electronic communication filtering technology where possible to protect ICT resources, limit access to inappropriate material or illegal activities (including in Library hotspots) and to assist users in managing nuisance emails.	Select devices users will be allowed to choose from.
	Monitor email for statistical purposes, user support, maintenance, security and investigative activities.	Update the list of devices every three months.
	Restrict access to library hotspots where there is evidence of excessive downloading of streaming data (e.g. movie downloads etc).	Keep records of all users assigned a CYOD, including: a. user's name, employee number, position and team; b. CYOD type, model, series number; c. date of CYOD assignment; d. date of CYOD return.
	Keep Council data and information secure. Privately owned and public library computers should not be connected to the business's network.	
	Remember the permanent storage of information is in the records management system rather than email boxes. Mailbox sizes should not be increased for users using inboxes as permanent storage.	
	Install new applications or transfer any executable file on the business's networked devices.	
	Liaise with other teams to discuss the need for requested software installation (for example, contacting GIS team regarding additional GIS software).	
	Support the installation of any networked photocopiers, printers and scanners from third party suppliers.	**Information Communication Technology**
	Purchase all software and hardware to be connected to business's network.	Organise the installation of fixed lines and data lines following user's leader approval.
	Only install trial software on the business's devices for evaluation purposes, and for a finite period of time.	Respond to user queries or any fault reports.
	Shut down all business computers at night to close sessions that have not been accessed for some time to help prevent unauthorised access to corporate data.	**Application, Back-ups Data Storage and Schedule Maintenance**
	Manage any devices connected to the corporate email Mobile Device Management (MDM) system.	Backup the business's ICT resources between 6pm and 6am.
	Except where otherwise approved, dual boot operating systems shall be used where a mobile device is also connected to the network. Depending on the situation this would normally only apply to network capable devices such as laptops or tablets.	Carry out monthly maintenance on all servers, and application maintenance as required.
		When possible, provide users at least 24 hours' notice where maintenance work needs to be carried out outside of business hours.
People Services	Inform the ICT Service Desk of any employee exits.	