General Policy

Policy Title: **Information, Communication and Technology**

Policy No: 209

Directorate: Corporate & Community Services
Responsible Officer: Manager Finance

Adopted Date: General Meeting – 15/04/2014
Review Date: 15/04/2016

VERSON	MEETING APPROVED	MEETING DATE	HISTORY
1	Policy & Strategy Meeting	03/06/2008	New Policy
2	General Meeting	15/04/2014	Policy Review

Authorities:

INTRODUCTION

These policies apply to all employees of the North Burnett Regional Council, and extend to other users who access the systems referred to within, including elected representatives, contractors, consultants, commercial business units and any other agents engaged by Council.

OBJECTIVES

This policy provides the foundation for the effective deployment and use of the North Burnett Regional Council's technology infrastructure, encompassing computer, network and communication resources.

It provides a minimum standard to which users must adhere to assist in the secure and efficient running of the North Burnett Regional Council's technology networks.

PRINCIPLES

The principles of this policy are described on the following pages, arranged by topic.

DEFINITIONS

- "Council" refers to North Burnett Regional Council.
- "Email" refers to electronic mail.

- "User" or "Users" refers to any user who accesses Council's systems or communication methods, including employees, elected representatives, contractors, consultants, commercial business units and any other agents engaged by Council.
- "Helpdesk" refers to system used to contact Council's IT staff.
- "Spam" or refers to any unsolicited email sent to a recipient, including advertising, phishing or otherwise malicious emails.
- "IT Officer" refers to Council staff employed in a role to implement or maintain Council's computer and communications systems.

COUNCIL PROVIDED MOBILE PHONES

Aim

To establish a minimum set of conditions for the use of mobile phones provided to designated users by Council to assist in the performance of their duties.

Policy

Subject to the following conditions and procedures, where designated by the Chief Executive Officer or General Manager, an appropriate mobile phone will be provided by Council to these users to assist in the performance of their duties.

Conditions and Procedures

Following are conditions and procedures relating to the use of mobile phones provided by Council:

1. The user shall ensure that due care is shown for the condition of the mobile phone. Handsets and supplied accessories must be kept in an "as new" condition.

2. Any damage or problems relating to the mobile phone shall be reported to the user's supervisor as soon as possible and an email sent to helpdesk for action.

3. The mobile phone should only be used for calls or SMS/MMS of a business nature. Where approval has been given by the Chief Executive Officer, non work related calls may be made, however the full cost of these calls will be charged to the user's debtor account and reimbursed. Users must advise a creditor's officer of any non-business usage to ensure charges are passed on.

4. Except where written advice is received from the Chief Executive Officer or a General Manager, the user is strictly prohibited to use the mobile phone to access services which attract a premium charge, including but not limited to "1900 numbers", "19 SMS services", Foxtel Mobile
5. Council's mobile phone services are arranged whereby calls between Council mobile phones are free. In order to save costs, where possible, calls between users should be made on mobile phones.

6. The mobile phone and accessories are to be returned to the designated user's supervisor upon termination of employment.

7. Mobile phones should be regularly charged and always switched on during the user's normal working hours or when on call.
8. All mobile phones must be set to silent mode upon entering Council's boardrooms.

9. Sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or otherwise inappropriate phone calls, messages or other communications are strictly prohibited from being transmitted, received or accessed using a Council mobile phone.

10. In collaboration with the Manager and Executive Leadership Team the IT section will settle upon a standard model of phone and accessories to supply to users. Differences in the equipment supplied may be allowed for certain groups of users at the request of the Managers, for example where benefits may be received for having certain features or capabilities in the handset.

11. Any damage or issues relating to the mobile phone shall be reported to the user's supervisor as soon as possible and an email sent to Helpdesk for resolution.

12. An IT officer will arrange the purchase and repairs of phones. Users are not permitted to undertake their own purchasing or repairs unless otherwise authorised by an IT officer.

13. Council utilises mobile device management services to monitor a wide range of mobile device attributes, including device location, and all mobile device users accede to having this information recorded. Users must not attempt to make changes to their handset or accessories that circumvent or attempt to circumvent this service.

14. Users are not to disable caller number display (caller ID) on mobile phones.

15. Personal use must be negligible and the user should make an effort not to be on a personal call for longer than is necessary. An excessive amount of personal calls made from a phone may result in the user being charged for those calls

COUNCIL FIXED LINE PHONES

Aim

To establish a minimum set of conditions for the use of fixed line phones provided to employees of Council to assist in the performance of their duties.

Policy

Subject to the following conditions and procedures, fixed line phones are installed by Council for users to primarily make and receive business related phone calls.

Conditions and Procedures

Following are conditions and procedures relating to fixed line phones provided by Council:

1. The user shall ensure that due care is shown for the condition of the unit. The handset is to be kept in a clean and "as new" condition. . Users are not permitted to write on the phone or apply any adhesive items such as stickers.

2. Users are responsible for all calls made from the fixed line phone available to them.

3. Personal use must be negligible and the user should make an effort not to be on a personal call for longer than is necessary. An excessive amount of personal calls made from a phone may result in the user being charged for those calls.

4. Any damage or problems relating to the unit will be reported as soon as practical to the user's supervisor and an email sent to Helpdesk.

5. In order to reduce call costs users should use the appropriate extension number to contact users in other offices where such an extension is available.

6. Users should answer a ringing phone within two rings if possible, and if the caller is unknown, answer with:

   "Good {morning/afternoon}, North Burnett Regional Council, this is {first name}"

7. Sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or otherwise inappropriate phone calls, messages or other communications are strictly prohibited from being transmitted, received or accessed using a Council fixed line phone. If a user received such a call, it should be terminated

8. Users must remain polite and courteous when using a fixed line phone, even when faced with adverse situations.

9. Fixed line phones provided in a Council residence are not subject to these conditions, however the tenant takes full responsibility for all communications using that phone.

10. Phones are not to be diverted to another user without their consent

11. Users are not permitted to disable caller number display (caller ID) on fixed line phones.

COMPUTER ACCESS AND USAGE

Aim

To establish a minimum set of conditions for the access and use of computer equipment provided to users by Council and to assist in the maintenance, security and stability of Council's computer network.

Policy

A desktop, notebook or tablet computer or personal digital assistant (PDA) shall be provided by Council to users who require one for business related matters.

Conditions and Procedures

Following are conditions and procedures of use relating to computer equipment provided by Council:

1. Users are responsible to notify Helpdesk in the event of any problems occurring with the equipment.

2. The user will ensure that due care is shown for the condition of all computer equipment. The computer must be kept clean of dust, and any vent holes must not be covered. Users must not apply magnetic or adhesive material, with the exception of a small amount of Blu-tack, to the equipment.

3. Council computer equipment must be predominantly used for business related tasks. Personal usage must be negligible and should not fall within designated work hours.

4. Users are responsible for any removable media used in their computer, and must ensure that such media is void of malicious or otherwise inappropriate files. Removable media includes CDs, DVDs, floppy disks and USB storage devices. If in doubt, a user should refer the media to an IT officer to be scanned.

5. Users must not change any computer system configuration except where advised by an IT officer.

6. Computers are not swapped or reallocated except at the request of, or permission from an IT officer. Laptop and tablet computers and PDAs are excepted from this condition, though permanent reallocation or relocation of those must be at the request of, or permission from an IT officer.

7. All computer equipment must be shut down at close of business each day to ensure updates and configuration changes are applied.

8. Due to Council's Citrix environment, users must log into one computer at a time.

9. Personal equipment may be connected to and used on Council's network with approval from the Chief Executive Officer or relevant General Manager. The IT department will attempt to cater for equipment, however may reject access under some circumstances.

10. Physical security and wellbeing of the computer is the responsibility of the user it is assigned to. Portable devices must travel as carry on luggage and not checked in luggage. Devices must be securely stored.

SOFTWARE ACCESS AND USAGE

Aim

To establish a minimum set of conditions for users to access computer software provided by Council to assist in the performance of their duties, and to maintain the security and stability of that software.

Policy

Council will endeavour to supply users with appropriate and up-to-date software.

Conditions and Procedures

Following are conditions/procedures of use relating to software on Council computers:

1. Users should advise their supervisor if additional or more up to date software is required to assist in the performance of their duties. The supervisor will liaise with an IT officer to seek to acquire the software.

2. Users are not permitted to install any software, programs or "apps" without permission from an IT officer.

3. Users are not permitted to change configuration options of software except where advised by an IT officer.

4. Users are not permitted to make any changes to the operating system configuration on their computer.

5. Any problems relating to software should be reported as soon as possible to Helpdesk for actioning.

6. Software installed on Council's computer systems is provided for business use only, and users are prohibited from installing any of their personal software without permission from an IT officer.

7. Council reserves the right to inspect or monitor any and all files or programs stored in all areas of its network, computer systems and any on-site or Council-owned removable media to ensure compliance with this policy.

8. Users are strictly prohibited from using computer software on Council computers to infringe copyright laws or access sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or inappropriate material in any way or form.

9. Council reserves the right to inspect or monitor any and all files or programs stored in all areas of its network, computer systems and any on-site or Council-owned removable media to ensure compliance with this policy.

10. All programs are to be closed before shutting down the computer.

11. Citrix programs must be used at all times. Use of locally installed programs is only permitted when working “offline”

12. Changes to permissions or access levels must be requested by a Manager by way of email to Helpdesk. No change requests from the user will be accepted.

EMAIL ACCESS AND USAGE

Aim

To establish a minimum set of standards under which users may communicate using Council’s email service to assist in performing their duties.

Policy

Subject to the following conditions and procedures, Council will provide access to its email service for users who have been designated to require such access. Each designated user is assigned a primary email address in the format *Firstname.Surname@northburnett.qld.gov.au*, and upon request, an additional generic email address, such as *positiontitle@northburnett.qld.gov.au*, may be enabled and redirected to the user’s primary address. Email addresses are not case sensitive.

Conditions and Procedures

Designated users are granted access to Council’s email service, subject to the following conditions and procedures:

1. Joke, humourous, sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or otherwise inappropriate images, audio, videos, documents or other files are strictly prohibited from being accessed, displayed, archived, stored, distributed, edited, recorded or printed using Council’s network or computing resources. Additionally, copyright material must not be transmitted where Council does not have the appropriate rights to do so.

2. Users are strictly prohibited from using Council’s email service to send unsolicited emails and those that may be construed to be political lobbying, or otherwise at odds with Council’s interests.

3. The user is responsible for ensuring only appropriate content is contained in emails.

4. Users must maintain due care and discretion when sending personal emails. Such emails must not contravene other conditions in this policy, and consideration must be given to the sensitivities of other users or external parties.

5. Council reserves its ability to monitor users’ email use where deemed necessary.

6. Council will automatically capture and preserve all users’ emails for the purposes of record keeping.

7. Email believed to be infected with a virus must not be opened, and must be reported to helpdesk as soon as possible.

8. Spam/bogus emails must be deleted upon receipt. Significant filtering is in place to reduce the number of spam emails. It should be noted that it will never be possible to block all spam emails.

9. Prior to forwarding a purported virus warning emails or other similar emails, users must consult with appropriate Helpdesk to determine if the threat can be substantiated.

10. Users are not permitted to change the font, stationery or their email signature. Council utilises a standardised email template and style to provide a consistent corporate image. Requests for changes to the title on the email signature must come from the Human Resources department.

11. Access to council email accounts on non council issued devices or through webmail services, is only permitted with prior approval from the relevant General Manager and IT staff. Requests may be denied due to technical, capacity or other reasons.

INTERNET ACCESS AND USAGE

Aim

To establish a minimum set of standards under which users may access the World Wide Web and other Internet services to assist in performing their duties.

Policy

Internet access is provided by Council to designated users within its networks, and may be extended to other locations such as libraries, or remote access services. Users are subject to the following conditions and procedures and must be responsible and exercise discretion in the use of the Internet to assist in performing their duties.

Conditions and Procedures

Users are granted access to Council's Internet services subject to the following conditions and procedures:

1. Sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or otherwise inappropriate images, audio, videos, documents or other files are strictly prohibited from being accessed, displayed, archived, stored, distributed, edited, recorded or printed using Council's network or computing resources. Additionally, copyright material must not be transmitted where Council does not have the appropriate rights to do so.

2. Users are strictly prohibited from deliberately performing malicious activities or using malicious programs including viruses, spyware, hack tools and other utilities that overload or disable computer system or network. Additionally, users may not access any tool intended to impinge upon the privacy or security of another user.

3. Except where provided by Council or authorised by the Chief Executive Officer, the use of chat rooms and instant messaging applications is strictly prohibited. Where allowed, such usage is bound by all applicable conditions in this policy.

4. Any use of peer to peer or other file sharing protocols or software such as BitTorrent, Internet Relay Chat or Gnutella is strictly prohibited. Additionally, users are prohibited from accessing binary newsgroups.

5. Users are aware that Council's Internet connection is not "unlimited", and agree to exercise discretion in the downloading of files from the Internet. Files greater than twenty megabytes should be advised to an IT Officer. Only files directly related to your role may be downloaded.

6. Personal use of Council's Internet services must be negligible and should not fall within designated work hours. If a user is requested not to use Internet services, they must disconnect immediately.

7. Council reserves its ability to monitor and log usage of its Internet services. , as well as blocking access to websites deemed inappropriate for use during working hours. The Chief Executive Officer or relevant General Manager may authorise access of any restricted websites.

8. Council reserves its ability to inspect, monitor or remove any file stored in all areas of Council's network, computer systems and removable media to ensure compliance with this policy.

9. If a user accidentally connects to a website or server that is in conflict of any of Council's policies, in particular item 1, they must immediately disconnect from it and advice Helpdesk.

10. Users are not permitted to download software.

SECURITY

Aim

To establish a minimum set of conditions for maintaining a high level of security and user-awareness for Council's computer and communications networks.

Policy

Users are responsible for maintaining vigilance and assisting in minimising the threat of a security breach to Council's computer and communications networks.

Conditions and Procedures

Users must assist in maintaining the security of Council's networks by adhering to the following conditions and procedures:

1. Users are responsible for all actions taken on a computer or other device or within software when they are logged into that computer, device or software.

2. If a user will be away from their computer for longer than thirty minutes, the user should lock their computer prior to departure. The lock function on a Windows-based computer can be quickly accessed with the key combination "⊞ + L".

3. Users must maintain passwords that are both strong/memorable only to them.

4. Passwords must not be shared between users by any means. In the event that a password is revealed, it must be changed as soon as possible in all relevant computers, devices or software. If IT staff are aware of users sharing passwords, a forced change of passwords will be done.

5. Users are not permitted to access Council's computer network under another user's account. Similarly, users without an account must not access Council's computer network under another user's account.

6. Password complexity must be of the standard enforced within Council's network.

7. Any potential or successful security breach must be reported to an IT Officer immediately.

8. Security codes must not be revealed to users other than those that require the code to perform their duties.

9. An IT Officer may be required occasionally to "crack" or guess a user's account or document password without the user's permission. When this occurs, the user will be advised and will be required to change the password as soon as possible.

10. Users are not permitted to access or attempt to access resources that aren't directly related to their role.

11. If incorrect security permissions are discovered on a resource, it must be reported to a supervisor immediately who will contact helpdesk to have the correct permissions applied.

VIRUS, SPYWARE AND MALWARE INFECTION PREVENTION

Aim

To establish a minimum set of conditions to assist in the prevention of virus, spyware and malware activity on Council's computer and communications networks.

Policy

By adhering to the following conditions and procedures, users will assist in minimising the threat that viruses, spyware and malware pose to Council's computer and communications networks.

Conditions and Procedures

Users must assist in the prevention of virus, spyware and malware infection by following these conditions and procedures:

1. Suspicious files must be reported to an IT Officer as soon as possible.

2. Users must not attempt to disable or uninstall any anti-virus, anti-spyware or antimalware software already installed on Council-provided computers and devices.

3. Any infection or genuine threat of infection must be reported to an IT Officer as soon as possible. Users should not continue to use infected computers or devices until it has been inspected by an IT Officer.

CONTACTING IT STAFF

Aim

To establish a standard and consistent means of contacting IT staff and logging jobs.

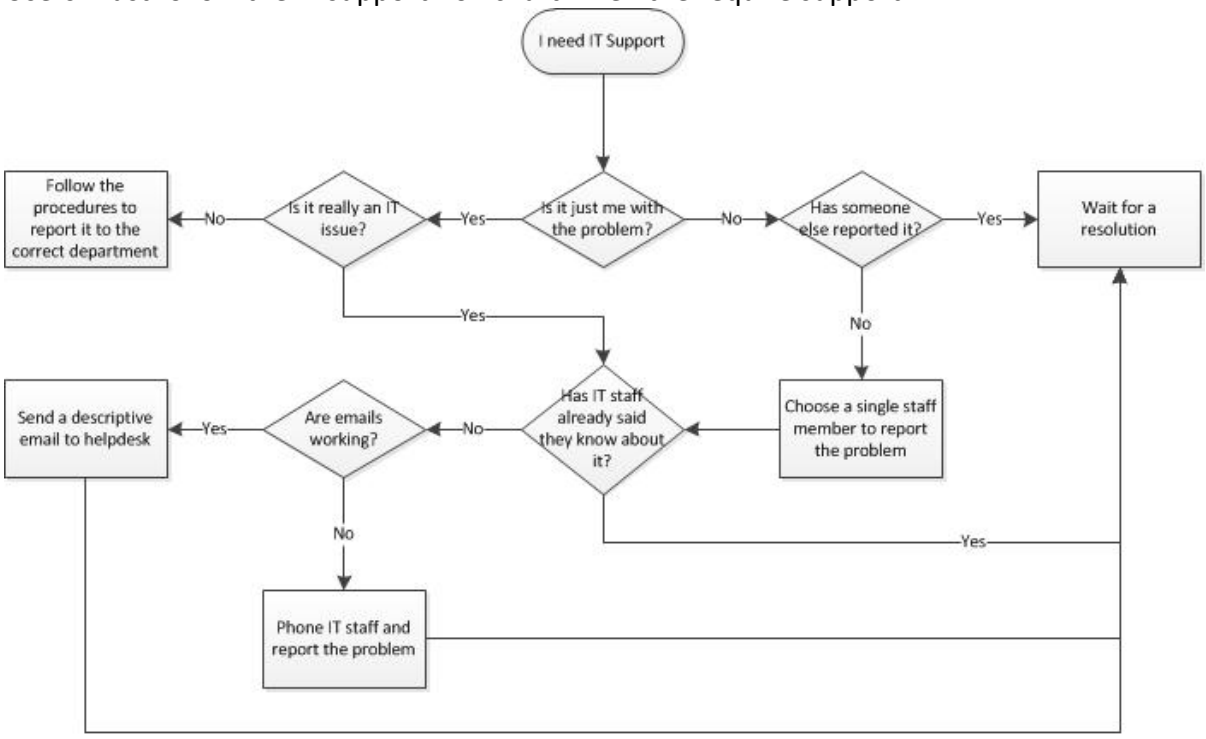
Policy

The IT Department utilise a job focused ticketing system known as "Helpdesk" to coordinate, schedule and manage all IT work. The system is an internal website which has an extensive email interface, allowing easy interaction with users.

Conditions and Procedures

Users are responsible for reporting all IT issue to Helpdesk for actioning, adhering to the following conditions and procedures:

1. Users must follow the IT support flowchart when the require support.



2. When reporting issues to Helpdesk, users should:
   - send only one email directly to Helpdesk, without any "CC";
   - provide detailed information, including any error messages and a screenshot if possible;
   - only send requests for assistance, not "FYI" messages;
   - ensure that you note in the helpdesk email if it is time sensitive/critical;
   - know that certain requests must come only from certain users (eg. position title changes or new employee requests from Human Resources, permission changes from the user's supervisor); and
   - do not leave issues until the last minute.

MICROSOFT LYNC

Aim

To establish a minimum set of conditions for utilising the internal Lync messaging, video conferencing and other functions in an efficient manner.

Policy

By adhering to the following conditions and procedures, users will assist in maximising the effectiveness and efficiencies provided by the Lync software.

Conditions and Procedures

Users are granted access to the Microsoft Lync software subject to the following conditions and procedures:

1. Sexually explicit, violent, racist, offensive, defamatory, harassing, illegal or otherwise inappropriate messages or other communications are strictly prohibited from being transmitted, received or accessed.
2. Users should either report work-related notes or leave the “what’s happening today” field blank.
3. Users understand that the use of Lync must be for work-related purposes and that all messages are recorded.
4. In order to assist users to identify each other, a “head shot” profile photograph of the user should be supplied to Helpdesk for application to the users’ account. The photo will be used as the user’s corporate photo and, among other places, will be displayed in Lync and Outlook.