GLEN INNES SEVERN COUNCIL

Computer Usage Policy

RESOLUTION NUMBER:	***11.05/17***	***MEETING:***	***25 May 2017***
	10.05/15		*28 May 2015*
	17.02/13		*28 February 2013*
	9.12/10		*16 December 2010*
	10.03/07		*22 March 2007*

Glen Innes Severn Council (Council) employees have a responsibility to be ethical and efficient in their official or authorised private use of Council's property and services, including computers and associated equipment, services and software.

To encourage the ethical, efficient and legal use of computer equipment, Council has prepared this Policy to identify and articulate obligations and standards that must be observed by employees when using Council's computers.

Aims

The aims of the Computer Usage Policy are to:

- protect Council's network infrastructure and software, confidential information, intellectual property, operating efficiency and public reputation;
- discourage or prevent unlawful behaviour arising from use of computers, including but not limited to harassment and discrimination,
- reinforce to computer users that Council's computer facilities are provided primarily for business use and that personal use, when permitted, is a privilege;
- provide users with clear rules and / or guidelines for computer usage that encourage ethical behaviour, efficient use of resources, and work productivity.

Legal Implications

Council and its employees / agents have a responsibility to comply with relevant laws when using Council property or information. Council must also comply with relevant legal provisions when monitoring or enforcing usage requirements. Applicable statutes include:

- *Local Government Act 1993;*
- *Privacy and Personal Information Protection Act 1998;*
- *Health Records and Information Privacy Act 2002;*
- *Independent Commission Against Corruption Act 1988;*
- *Government Information (Public Access) Act 2009;*

- *State Records Act 1998;*
- *Workplace Surveillance Act 2005; and*
- *Anti-Discrimination Act 1977.*

APPLICABILITY

This Policy applies to all authorised users of Council's computer systems, including staff, councillors, contractors and, where applicable, volunteers.

Use includes, but is not limited to, sending and receiving emails, accessing the Internet, using electronic media, access to and use of network systems, use of all desktop or laptop computers, use of all mobile devices that access Council's computer network or the Internet (for example, tablet computers and "smart phones"), and access to and use of all applications and data.

Council computers, mobile devices and all associated software and hardware shall be used strictly in accordance with the Glen Innes Severn Council Computer Usage Policy and associated Protocol and Procedures.

IMPLEMENTATION / COMMUNICATION

This Policy will be communicated to all new employees that are affected by it as part of their induction. Revised versions of the Policy that contain significant changes will be communicated to all relevant staff by Human Resources staff. New versions that only contain minor or inconsequential changes will be distributed to managers for highlighting at team meetings.

VARIATION AND REVIEW

This Policy shall be reviewed every three (3) years, or earlier if required. Council reserves the right to vary or revoke this Policy at its discretion.

General Manager

31-5-2017

Date

Reference Number:	Version Number: 5 Date of Effect: 25/5/17	Review Date: May 2020	Responsible Officer: Manager Admin and HR
Related Documents: Records Management Procedures and Information Manual			

GLEN INNES SEVERN COUNCIL
COMPUTER USAGE POLICY (PROTOCOL AND PROCEDURES)

Acceptable Use of Council's Computer Facilities

All Council computer facilities, including email and Internet accounts and the data and messages contained within or transmitted via them, are Council's property and are primarily intended for business use only.

All users are advised that they do not have any personal or proprietary rights over such facilities or accounts. Council cannot guarantee the privacy or confidentiality of any information stored or sent internally or via the Internet.

Council may provide any user who has access to Council's computer network with an internal email account, at Council's discretion.

Users will not be granted access to and use of Council's Internet or email communication facilities unless an Internet and Email User Agreement (refer **Appendix 1**) has been signed by the user.

After access and use has been granted, use of Council's computer facilities must be appropriate, lawful, efficient, professional and ethical.

Use of Council's computer facilities shall at all times comply with anti-discrimination laws, workplace relations laws, Council's Code of Conduct and Workplace Discrimination and Bullying / Harassment Policy, and other relevant laws or policies.

Except as set out in this Policy, Council's computer facilities may only be used for purposes consistent with the normal daily business operations of Council, including, but not limited to:

- Retrieval and distribution of information, technical materials, support documentation or promotional material that may assist users in their daily business operations; and

- Normal administration and support activities.

Reasonable private use of Council's computer facilities, particularly Internet and email, may occur during an employee's private time (e.g. lunch break) provided it is without detriment to a user's work or the business of Council, does not create an unfavourable impression with customers and does not contravene any prohibited use set out in this document.

The user also acknowledges that although all attempts are made to protect Council's computer network from being infected by malware (for example, computer viruses, Trojans, worms, spyware, rootkits, keyloggers) and other malicious code, these forms of software may be present. Council takes no responsibility for personal information that may be damaged or lost as a result of malicious code.

Prohibited Use of Council's Computer Facilities

The following activities in relation to the use of the Council's computer facilities are expressly prohibited.

- Using Council's computer facilities (including email or the Internet) to store, request, access, transmit or convey images, content or materials that:
  - are fraudulent, illegal, offensive, threatening, abusive, defamatory or may constitute harassment;
  - are likely to contain any malware or other malicious code;
  - violate Council's Code of Conduct and / or any State or Commonwealth Act of Parliament;
  - contain another person or company's trademarks or copyrighted materials without specific authorisation to do so from the owner of the trademark or copyright;
- Sending or forwarding any 'chain' letters or 'hoax' e-mails.
- Using Council's computer facilities to solicit outside business ventures or with a view to personal profit or gain.
- Using Council's computer facilities to store, distribute, download, install or otherwise utilise any software in a manner that is inconsistent with the software's licence agreement.
- Using Council's computer facilities to harass, abuse, intimidate or interfere with others in a malicious manner.
- Using Council's computer facilities to gain (or attempt to gain) unauthorised access to Council's or any third party's data, databases, servers or networks or breaching any security measures on Council's or any third party's system.
- Using Council's computer facilities to intercept (or attempt to intercept) any data transmissions without authorisation.

- Using Council's computer facilities to download any executable software applications or utilities from the Internet or other source without approval from Council's Network Administrator * (except when done unintentionally).

- Intentional disclosure or swapping of user logins / passwords that have been set up to safeguard the security of the computer network, individual computers or applications. If access is required, users are to contact the relevant system administrator (Practical Plus / Enterprise Content Management, MapInfo, etc).

- Using Council's computer facilities to intentionally create, send, access or store information that could damage or embarrass Council, its employees, agents, members of the public and other stakeholders.

- Using Council's computer facilities to intentionally create, send, access or store information that could be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory.

- Using Council's computer facilities to transmit, communicate or access any material that may unlawfully discriminate against, harass or vilify colleagues or any member of the public on grounds including but not limited to sex, sexual orientation, race, colour, nationality, descent, ethnic or ethno-religious background, marital or domestic status, disability, pregnancy, age, infectious disease (including HIV/AIDS), transgender status, or responsibilities as a carer.

Users who aid and abet others in unlawfully discriminating against, harassing or vilifying colleagues or any member of the public may also be held personally liable for such actions.

**** For the purposes of the Computer Usage Policy and Procedures, the Network Administrator is Council's Manager of Administration and Human Resources or other Council officer who has been delegated the role of Network Administrator.***

Email Format / Disclaimer

Email messages sent from Council's network project Council's corporate image and accordingly are to follow a standard format. Messages are not to include non-standard borders or backgrounds, emoticons ("smiley faces", etc), non-standard commercial images / promotional material, or other unauthorised items. Due to electronic record keeping requirements, electronic business cards cannot be used.

A standard disclaimer will appear at the bottom of all outgoing emails sent from Council's facilities. This disclaimer will, by default, appear unless deliberately disabled by the Network Administrator. Users must not delete or amend the disclaimer, which is to be automatically attached to all outgoing emails:

Glen Innes Severn Council NOTICE & DISCLAIMER

The information contained in this message and or attachments is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. If you received this message in error, please contact the sender and permanently delete the message and its attachments.

The opinions expressed in this message are the personal views of the sender and do not necessarily represent the corporate opinions or policies of Glen Innes Severn Council, unless expressly stated.

Record Keeping

Email messages and their attachments are corporate records if they document Council's business and activities and need to be retained as evidence of those actions.

All corporate records, irrespective of their form or substance are required to be retained in a manner and for a period that complies with the requirements of the General Records Disposal Schedule for Local Government.

Corporate records include, but are not limited to the following:

- Working papers detailing development of reports and documents;
- Final versions of reports;
- Policy documents and statements;
- Formal minutes of Council Meetings and its Committees;
- Formal communications between Council Officers;
- Formal communications between Council Officers and external agencies, organisations or individuals.

Email Received at Council's Official Address (council@gisc.nsw.gov.au)

All email received at Council's official address will be dealt with in accordance with records procedures for the receipt and handling of incoming mail.

The Records Supervisor is responsible for opening the email and determining whether the item requires registering or otherwise.

Should the Records Supervisor determine that the item requires registration, the message and its attachments will be registered and then forwarded electronically to the appropriate Council officer for information / action.

Should the Records Supervisor determine that the item does not require registration, the message shall be forwarded to the appropriate officer electronically, without registering it.

Email Received by a User

Email received by an individual user will either originate from an external source or internally.

Email received by a user from an external source must be registered into the appropriate record keeping system if items received relate to a business activity of Council.

Email received internally that does not constitute "official" correspondence, will be the responsibility of each staff member to deal with accordingly.

Council's email system should not be used as an indefinite additional storage space. If email messages are records that must be kept indefinitely, they are to be registered into Council's appropriate record keeping system and deleted from the Outlook folders.

A maximum of 600 megabytes will be allowed for storage of emails, calendar information, contacts and any other folder information created within Outlook folders. Users who do not delete unwanted information and exceed this limit will not be able to send emails until the required limit is met.

Retention and Management of Email Corporate Records

As with paper records, the custody and disposal of electronic records is the responsibility of the Records Supervisor.

Internal and external email that meets the criteria for corporate records must be registered and stored in the appropriate record keeping system. If the email recipient is unsure whether an email message meets the criteria for a corporate record, the email should be referred to the Records Supervisor for evaluation and advice.

Legal Issues

Legally, email and electronic file notes have the same standing in court as paper documents. The laws of Copyright, libel, discrimination and trafficking in prohibited goods and services can be applied to email and any attachments.

Care should always be taken to ensure that email messages and electronic file notes contain nothing that could bring Council into disrepute or subject it to legal action.

Although a user may delete his or her email, deleted messages can be retrieved and submitted as evidence in legal and / or disciplinary proceedings.

Web Browsing and Use

Council's Internet connection is protected via a firewall device prohibiting unauthorised access from external sources via the Internet.

Users should be aware that non-authorised freeware and plug-ins, such as Internet browser search bars, anti-spam plug-ins, and free anti-virus products, might in fact be malware or contain other malicious code masquerading as legitimate products.

Although Council's network is protected by a firewall and Internet security software, no executable files (which include *.exe, *.com, *.bat, *.zip), screensavers, browser plug-ins, email client plug-ins, etc, are to be downloaded or installed on individual devices without the specific authorisation of the Network Administrator.

Downloading and / or installation of essential updates, upgrades, plug-ins, extensions, etc, for previously authorised Council software, is permissible without further authorisation. A list of authorised software is included at **Appendix 2**.

No streaming media is to be intentionally accessed except for essential work purposes. This includes video, audio (Internet radio stations etc). Such downloads include large amounts of data and will degrade Internet connections and performance.

Chat or Instant Messaging access or software is not permitted, except where authorised for work purposes. Such programs require the opening of "ports" on the firewall in order for these software packages to operate. This will lessen the security of Council's internal network, making it vulnerable to security risks.

All social media access and use (for example, Facebook, LinkedIn, YouTube and Twitter) is to be strictly in accordance with Council's Social Media Policy.

All users should be aware that Internet use is primarily for work purposes and that excessive or unreasonable private use is not permitted. Private use during work hours is also not permitted, except where specifically authorised, eg, under Council's Study Incentives Policy.

Council uses monitoring software to actively monitor the web-browsing gateway for bandwidth / download usage of individual workgroups and users. Such software also has the capability to monitor Internet / email content if necessary. Anomalous usage patterns will be reported to the relevant manager / supervisor to be taken up with the user(s).

Users must acknowledge that their web browsing may be monitored and / or reported on and their access to the Internet will not be activated until they have read this policy and agree that they fully understand its terms and conditions.

Monitoring of Council's Computer Facilities and Information

Council reserves the right to conduct surveillance whether by way of monitoring, copying, accessing or disclosing any information or files that are stored, processed or transmitted using Council's computer facilities. This includes documents, files, email messages sent by users internally or externally or received by users, and Internet activity.

Subject to the *NSW Privacy and Personal Information Protection Act 1998*, users of Council's communication facilities should not have an expectation of privacy for any actions performed using such facilities, including personal email, messages, files, documents and other data created, deleted, sent, received and / or stored.

Users should be aware that emails, messages, files, documents and other data might be archived by Council management, as it considers appropriate. In addition, emails, messages, files, documents and other data that has been deleted may continue to exist in the Council's backup systems.

Council reserves the right, at any time, to monitor, copy, access or disclose any information or files that are stored, processed or transmitted using Council equipment and services.

Council may monitor its communication facilities on a random or continuous basis to:

- intercept and stop emails using a range of different tests (for example, emails believed to contain malware, emails containing .exe file attachments, emails larger than a pre-defined size, etc);
- prevent de-standardisation of the computer network due to the downloading or deployment of unauthorised software or hardware;
- ensure compliance with Council policies and procedures;
- investigate conduct that may be illegal or adversely affect the Council or its employees; and
- prevent inappropriate or excessive personal use of Council Internet and email facilities.

If an email message is intercepted, the user sending or receiving the email will be notified of the prevented delivery of the e-mail, unless:

- the email is considered to be 'Spam';
- the content of the email might have resulted in an unauthorised interference with or damage to a computer or computer network or any programs run or data stored on the computer or the computer network; or
- the email would be considered by a reasonable person to be menacing, harassing or offensive.

Council may change the criteria for intercepting and stopping emails at its discretion. Such changes will be notified to all users before implementation.

The user, by signing the Internet and Email User Agreement, waives the requirement that electronic surveillance cannot commence prior to a 14 day notice period. The user also acknowledges that his / her Internet / email usage is continuously monitored by Council for the protection of Council's computer network.

Breaches of this Policy / Protocol

Users who are suspected of violating any of the provisions of this policy may be subject to disciplinary action in accordance with Council's Unsatisfactory Performance/Disciplinary Procedures Policy. Such disciplinary action may include, but is not limited to:

1. Suspension of computer privileges;
2. Counselling / formal warning;
3. Admonishment or reprimand;
4. Demotion to a lower grade either permanently or for a period to be determined;
5. Suspension from duty with or without pay for a specific period;
6. Dismissal, including summary dismissal, for gross misconduct or where continual breaches and counselling have failed to resolve the matter (consistent with the relevant award and legislative requirements).

Users should also be aware that Council is required to report any criminal and civil law violations to the appropriate authorities.

APPENDIX 1

GLEN INNES SEVERN COUNCIL

INTERNET and EMAIL USER AGREEMENT

I, _____ acknowledge that I am being granted Internet and / or email access using Glen Innes Severn Council's computer facilities in order to carry out my employment duties.

Users' Responsibilities

By using the Council's computer facilities, I accept responsibility to comply with its Computer Usage Policy and all associated rules and procedures, which I have read and understand.

I acknowledge that any inappropriate use of the Council's computer facilities may be investigated and may be subject to disciplinary action, including termination of my employment and / or any civil or criminal legal action.

I agree that my use of these services and facilities will be in strict accordance with Council's Computer Usage Policy. I also acknowledge that I have read and understand the content of Council's Computer Usage Policy and that by signing this Internet and Email User Agreement:

1. I have been given notice in accordance with section 10(2) of the *Workplace Surveillance Act 2005 (NSW)*; and

2. that Council will be entitled to, and shall commence monitoring, all my personal / business use of these services and communication facilities, and

3. that monitoring will be in accordance with Council's Computer Usage Policy.

I understand that if I am not prepared to accept any of these conditions that access to external email and Internet facilities will NOT be granted.

User Signature: _____ Date: _____

User Name: _____

Witness Signature: _____ Date: _____

Witness Name: _____