



# *Muswellbrook Shire Council*

---

## Computer and Information Technology Use

Policy No. C51/1



**Written by  
Shane King  
IT Manager**

**Adopted By Council  
10 September, 2007  
Minute No. 155**

## **Computer & Information Technology Use**

### **C51/1**

#### **1 Definitions:**

##### **1.1 Information Technology Resources:**

Means computer equipment, including personal computers, scanners and printers, including those connected to any council network, email, facsimiles, internet, intranet, mobile telephones, pagers, telephones, two way radios, digital cameras and blackberries.

This definition will be automatically updated as technology is added to the resources.

##### **1.2 Users:**

Means Councillors, members of council staff, work experience students, casual and temporary staff, contractors, consultants, volunteers, members and community representatives on council advisory committees and community groups given permission, in writing, to use council's information technology resources by the General Manager

#### **2 Objective:**

##### **2.1 To provide users with operational guidelines in the use of information technology resources as provided by Council. The Policy applies to all users.**

Note that this policy is to be read in conjunction with MSC001-Council Computer Information Guide

#### **3 Uses:**

##### **Proper Use:**

##### **3.1 Muswellbrook Shire Council provides information technology resources to enable its users to do business in an ethical, effective, efficient and careful manner. Users are reminded that they must observe the council's Code of Conduct.**

##### **Improper use:**

##### **3.2 Users must not use information technology resources to search for, access, download or communicate any improper material. Improper material is material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature.**

##### **Responsibility of users**

##### **3.3 Users will be notified of amendments to this Policy; however it remains the responsibility of the individual to ensure they are familiar with the contents of this policy, and future amendments.**

#### **4 Security:**

- 4.1 Each user that is required to use any of Council's Computer systems will be issued with a logon ID and password and no user is to divulge their logon ID or password to another user or to persons outside of Council.
- 4.2 All information, data or files created by you while using Council's information technology resources employed by the Council are subject to scrutiny. It is important to remember that data files are official documents that are subject to the same laws as any other form of correspondence. They are subject to statutory record keeping requirements and can be subpoenaed or "discovered" during legal processes.
- 4.3 The requirements of the State Records Act and associated policies must be observed.
- 4.4 The Council may access or disclose private electronic messages or files of an employee with good cause, provided that it follows appropriate procedures designed to assure compliance with Council policies. Good cause shall include the need to protect system security, fulfill Council obligations, detect employee wrongdoing, comply with legal process, or protect the rights or property of the Council.
- 4.5 PC's should be logged off at the end of day or when last used for the day, to prevent unauthorised use after hours.
- 4.6 Email should not be used for highly sensitive or confidential information, unless appropriate actions are taken to secure the contents against disclosure, alteration and forgery.

#### **5 Information:**

- 5.1 Information produced by users that is created as part of their duties, is not to be released to external bodies without approval from Departmental Directors or Managers or the General Manager, or unless its release is covered by Legislation or Policy governing its release.
- 5.2 Users should consider the sensitivity of information that exists in electronic form, when sharing this information with other employees of Council. Users must not use information contrary to Council's Code of Conduct, Privacy Management Plan and Privacy Legislation.
- 5.3 Users should consider record keeping requirements when choosing a means to communicate information. Some methods such as SMS and instant messaging will not provide evidence that record keeping requirements are being met and should not be used.
- 5.4 Users should not use Council email or electronic messaging systems to distribute improper material, fraudulent or harassing messages, to infringe the copyright or other intellectual property rights of third parties, or otherwise to engage in any illegal or wrongful conduct.
- 5.5 The Council reserves the right to audit and remove any illegal material from its information technology resources without notice.

5.6 Messages conveyed by E-mail and through the Internet are capable of being intercepted, traced or recorded by others. Although such practices may be illegal, users should not have an expectation of privacy and must take care with confidential documents.

5.7 Users who have technology provided by Council that provides remote access to Council, are to ensure the resource is used only by those so authorised.

## **6 Access to the Internet:**

6.1 Access will be granted based on the identification of a genuine business need with approval from the Department Director and IT Manager. By requiring approval from both parties, Council is placed to ensure its use meets a business need, and does not sacrifice capacity or security of Council's information technology resources.

6.2 Any user with Internet access will connect through Council's gateway to ensure use of Council's firewall and security features. Additional connections to Internet providers are prohibited unless approval has been obtained from the IT Manager.

6.3 Examples of unacceptable use of the Internet include, but are not limited to, the following:

- Using Council Internet access for personal commercial purposes.
- The viewing, downloading or re-distribution of improper material.
- Downloading of information if this will breach copyright legislation.
- The playing of games over the Internet and the downloading of games or video footage from the Internet.

## **7 Personal Use:**

7.1 Council accepts some personal use of the information technology resources may occur. Users are advised to limit the amount of personal use so as not allow it to impact on their normal duties.

7.2 When considering personal use, the user should use discretion and ensure it remains within the guidelines set in this policy.

7.3 Reasonable private use of the systems provided by Council is a privilege and such use needs to be balanced in terms of the Council's commitment to meeting operational needs.

7.4 The home directory for each individual is not to contain excessive quantities of non business related material.

7.5 Examples of limited personal use would include

- Internet browsing in the employee's lunch break, which could include access to banks for bill payment and the like. This would require the Managers approval, and be within guidelines as listed in this Policy
- Personal emails that require no more than 5-10 minutes of an employees time per day
- No more than 5 MB of files stored in the employees Home Directory

7.6 Councillors who are issued with Council facilities such as fax machines and phone lines should limit personal use of these facilities. Councillors are reminded of Council's Code of Conduct, its Key Principles (Section 4) and General Conduct Obligations (Section 6)

7.7 Personal use will always be at the General Manager's discretion.

## **8. Mobile Phones**

8.1 Personal use of mobile phones must be paid for by the user and should be restricted to calls of an urgent nature. Users are however reminded that mobile phones are provided to aid the employee in conducting council business, and are not provided as a personal accessory outside of Council business. Users who require mobile coverage outside of work business should purchase their own phone.

8.2 SMS capability on Mobiles will be granted based on the identification of a genuine business need and require approval from the Department Director.

8.3 SMS is not a valid form of communication by Council staff, as it does not comply with record keeping requirements.

8.4 Staff and Councillors who are issued with Council mobile phones are not to use the devices inappropriately. Users should not download ring tones, subscribe to message services, nor use the device to store or send items such as pornographic messages or images.

## **9 Logging of Activity:**

Council reserves the right to, and may, monitor activity for the purpose of:

9.1 Monitoring the levels of demand of the technology, and use this information in planning for future needs.

9.2 To ensure usage of information technology resources is within Council guidelines and to identify any unauthorised use.

## **10 Software:**

10.1 Software considered necessary by Council to enable users to carry out the roles and responsibilities, will be provided by Council.

10.2 Software installed on Council's information technology resources must possess a License, permitting its lawful installation and use.

10.3 Users are not permitted to install software other than that provided by Council. This includes software from Home, Sales Personnel, and Consultants.

10.4 Should a program need to be installed for the purpose of evaluation, then the IT section is to be contacted. If software is to be downloaded at the instruction of a supplier, then it should be referred to the IT section.

10.5 No copying of Council software is permitted, and users found to be in possession of copies of Council software may be the subject of disciplinary action or forfeiture of rights to use the information technology resources

10.6 Users must not use software or systems that provide those users the ability to “Sniff” or monitor network traffic, unless part of a sanctioned activity. Users caught using such technology may be subject to disciplinary procedures or forfeiture of rights to use the information technology resources.

## **11 Hardware:**

11.1 No hardware may be removed from council premises without written permission from the relevant Manager.

11.2 No hardware or software (including portable equipment) will be loaned to persons, other than members of council staff, unless prior approval in writing is obtained from the Department Director.

## **12 Data Retention**

12.1 Files created in the day-to-day Council Business are to be stored on Council Servers to ensure the data is secured by suitable means and is included in backup and archive methods as provided by Council.

12.2 Retention and Storage of data should be in accordance with procedures as set down under the State Records Act.

## **13 Contractors and Community Groups**

13.1 All users, other than members of council staff, are **not** permitted to connect PC’s, laptops, servers and the like, to Council’s Local Area Network or Wide Area Network, without prior approval from the IT Manager. This includes and is not limited to, direct connection or connection via dialup.

13.2 Managers who identify a need to have such a facility must obtain approval from the IT Manager for the third party to connect. This is to protect Muswellbrook Shire Council’s investment in technology and no exceptions should be considered due to the risk potential.

13.3 An audit of the third party equipment will be conducted prior to approval, and repeated at regular intervals dependant on the duration of the activity. Long durations will require monthly audit of non Council equipment ensuring;

- Antivirus Software owned by the third party is current
- That the equipment is not configured in such a way that may adversely affect Councils information technology resources.
- That no equipment contains network sniffers, data packet capture software, password cracking utilities and the like.
- That the equipment that has approval is the only equipment being used and has not been substituted.

## 14 Reporting Breaches

Users are encouraged to report breaches of this policy to their supervisor or an appropriate senior officer or the General Manager. All use should be consistent with the Council's Code of Conduct, which also has guidance on reporting misuse of public resources.

\*\*\*\*\*

### Additional Reference

#### Computer - Virus Protection Policy

#### REVIEW HISTORY:

	<i>Current</i>	<i>Previous</i>	<i>Prior</i>	<i>Prior</i>
<i>Minute No:</i>	155	195		
<i>Meeting Date:</i>	10/09/2007	20/06/2005		
<i>Review Date:</i>	September 2009			
<i>Rescind Date:</i>				