

USE OF COMMUNICATION AND INFORMATION TECHNOLOGY DEVICES

PREFACE

We aim to be an effective organisation. The implementation of best practice management systems that foster a cooperative and productive workplace and ensure the effective use of available resources is one way of achieving this. As a public sector agency, we must be efficient, economical and ethical in our use and management of public resources provided for business purposes, including devices such as telephones, email, USB drives and PDA's.

In addition, we are committed to providing a service that is accessible to everyone, to act conscientiously and competently, and to treat individuals and agencies courteously, attentively and sensitively. This in particular affects the way we use communication and information technology devices.

PURPOSE

The purpose of this policy is to set out the responsibilities of staff when using communication and information technology devices, to inform staff of the systems in place to monitor use of communication and information technology devices, to address certain security issues and to provide guidance on the status of emails as official records of our business activities.

RESPONSIBILITY

This policy applies to the Ombudsman and all staff of the office, whether by way of appointment, secondment, contract, temporary arrangement or on a fee-for-service basis. Any individual having employee functions or acting in an employee capacity, including a volunteer, is a member of staff for the purpose of this policy.

The Security Committee or Manager Corporate may make procedures, templates or guidelines supporting this policy. Staff will also be bound by these.

LEGISLATIVE/POLICY FRAMEWORK

The *Ombudsman Act 1974* and the *Workplace Surveillance Act 2005*.

Policy and guidelines for the use by staff of employer communication and information technology devices issued by the NSW Premiers Department.

NSW Ombudsman information security framework and associated policies, including the NSW Ombudsman Code of Conduct.

NSW Ombudsman policy number:	19
Policy originally created:	16 December 1999
Last reviewed / updated:	16 January 2006
Version number:	7
Related policies:	Code of Conduct, Information Security Policy, Disclosure of information, Records Management Policy

This policy supersedes the policy on Use of Communication Devices implemented on 17 August 2005.

DEFINITIONS

Communication or information technology device includes, but is not restricted to the following devices:

- **Computers** include, but are not limited to, desktop or portable computers or servers connected to any network
- **Electronic data interchange** or electronic document interchange refers to the application-to-application exchange of computer-based information over a data circuit
- **Email** (also known as electronic mail) refers to a computer-based message sent over a communications network to one or more recipients. It may be transmitted with attachments such as electronic files containing text, graphics, images, digitised voice, digitised video or computer programs.
- **Facsimile** refers to a communication device that converts each picture element of black and white into an electric signal. These signals in turn generate a constantly changing electrical signal that is transmitted on a data circuit (or telephone line) to a receiving facsimile.
- **Internet** is a world-wide loose affiliation of interconnected computer systems (involving government, commercial, academic and hobby providers) through which an individual with a personal computer can access services and information. Services available through the internet include, but are not necessarily confined to, electronic mail, Telnet and the World Wide Web (www).
- **Intranet** is an internal (restricted) network that uses internet technology. It is accessed over a personal computer.
- **Pager** refers to a small telecommunications device that receives (and in some case sends) short radio messages (either numeric or alphanumeric) and is generally used by people who are continually changing their location. When a pager captures a message it is usually accompanied by a beep to alert the person carrying the pager. Also known as a 'beeper'.
- **PDA** (personal digital assistant) refers to a handheld computer that serves as a mobile organiser and allows data such as email, outlook calendar appointments and contacts to be accessible while away from the desk. Data is synchronised between the PDA and desktop computer via a synch cradle. Only PDA's authorised by the office may be used on the office network. Staff must comply with procedures supporting this policy when using an office PDA.
- **Radio** refers to wireless electromagnetic means of point to many point communications.
- **Telephones** include, but are not limited to, hard-wired desk telephones, cordless telephones and mobile (cellular) telephones.
- **USB drive** refers to a small, portable flash memory stick that plugs into any computer's USB port and functions as a portable hard drive. A USB drive is small enough to be carried in a pocket and allows data to be easily transferred from one machine to another. Also known as 'flash drive', 'pen drive', 'keychain drive', 'USB key' and 'memory key'. Only USB drives authorised by the office may be used on the office network. Staff must comply with procedures supporting this policy when using an office USB drive.

Note the *Workplace Surveillance Act 2005* makes reference to camera surveillance and tracking surveillance (eg GPS device). At present we do not use such devices.

POLICY STATEMENT

1. Access to communication and information technology devices

All access to communication and information technology devices owned or used by the Ombudsman is subject to this policy. Only members of staff who have made a written undertaking that they have read

and understand this policy or who have previously signed the office's policy on use of communication devices will have access to communication and information technology devices.

Access to the office's internet service provider accounts must only be through authorised office equipment located in the office.

You may only access an office mobile telephone if it has been allocated to you by the Ombudsman or his or her delegate as necessary for the performance of your job, or otherwise in accordance with the specified procedures.

You may only access an office portable computer in accordance with the specified procedures.

2. Monitoring of use

Communication and information technology devices are provided by the office for work-related purposes. While reasonable private use is authorised (please see the section in this policy on economic use), personal use of these devices will be subject to the same level of scrutiny as work-related use.

All information, data or files created by you while employed by the office are subject to scrutiny. Electronic messages are official documents that are subject to the same laws as any other form of correspondence.

The office may monitor, copy, access or disclose any information or files that are stored, processed or transmitted using agency equipment and services. The office may monitor email and internet use by staff on a random or continuous basis to:

- prevent de-standardisation of the computer network because of the downloading of unauthorised software
- ensure compliance with office policies
- investigate conduct that may be illegal or adversely affect the office or our employees, and
- prevent inappropriate or excessive personal use of office property.

Mail filtering is necessary to protect the office computer network from constant threats in the form of emails. These include viruses and spam. All inbound emails are monitored automatically by software. Emails determined to be spam, to contain viruses or files that are potentially dangerous to internal networks are blocked. IT staff manually check blocked emails to determine their appropriateness for release. Employees will be notified of blocked emails unless they are believed to be spam or to contain viruses. IT staff must comply with procedures supporting this policy when monitoring and releasing blocked emails.

Staff internet use is monitored automatically by software. Each website is pre-scanned to determine if it contains pornography, otherwise offensive material or content dangerous to internal networks. In addition, the software continually monitors staff internet use which is then used to conduct periodic random audits. The office may conduct ad-hoc audits of individual staff at the request of a statutory officer or team manager. Audits include reviewing visits to offensive and inappropriate sites, and whether levels of personal internet use are inappropriate.

All inbound and outbound telephone calls are monitored continually by software. Reports may be used to isolate or identify problems with the switchboard, or to identify or monitor abusive or inappropriate calls. Reports may also be used at the request of individual staff to identify personal calls for the purposes of staff contribution.

Supervisors intermittently monitor inquiries staff work-related telephone calls for induction and training purposes. This is not done without the officer's knowledge and consent.

Any calls that are made on an office mobile telephone will be recorded on the telephone bill. Mobile telephone expenditure must be reviewed and approved by a team manager or a statutory officer.

The office monitors after-hours staff access to office premises, and 24-hour access to high security office areas.

3. Economic use

Computer equipped workstations and the services accessible on them, mobile telephones, portable computers, PDA's and USB drives are provided to staff for business use to carry out tasks related to your job. Reasonable private use of the internet and email is a privilege and needs to be balanced in terms of the government's commitment to the development of a responsive and flexible public sector, and operational needs.

(a) Telephones

Where possible and appropriate, members of staff are encouraged to use free-call telephone services. These generally provide more economical and efficient means of communication. Because all calls involving a mobile telephone are time charged, staff members should keep short any communication involving a mobile telephone. This applies equally to calls made from standard desk telephones as well as call from mobile telephones. Calls involving mobile telephones should be avoided where standard desk telephones are readily available.

(b) Email

While email may be used for official communication purposes, you should continue to send written correspondence by post where this would be ordinary procedure. Email may be used where it is the requested form of communication by external parties and/or where the efficiency of inquiries, investigations or other business would be facilitated by the use of email.

Any communication sent by email should also be in accordance with general office procedures and your level of delegation for the sending and signing of correspondence and any supervision approval requirements that apply.

(c) Internet

All use of the internet must have a clearly defined purpose at the outset of any session. If you are accessing the internet from a standalone computer, you must remember to log off before leaving the workstation. You should be mindful that standalone computers are a resource to be shared with other staff members and use them only for as long as necessary.

4. Lawful and ethical use

It is not acceptable to intentionally create, send or access information that could damage the reputation of the office, 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.

Inappropriate use includes, but is not limited to, any use of equipment or services of the office for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.

If you receive and open an email that contains pornographic or sexually explicit material, images, text or other offensive material, you must immediately:

- forward the email to the IT Manager or Manager Corporate, who has responsibility for monitoring email and internet use by staff
- reply to the sender of the email indicating that the material is inappropriate, that the message will be deleted and that no further communications of a similar nature should be sent to you
- delete the email from your *Inbox*, *Sent Items* and *Deleted Items*.

It is inappropriate to transmit, communicate or access any material, which may discriminate against, harass or vilify any person with whom you have business dealings, including a colleague or any member of the public.

In particular, it is unlawful to do this on the grounds of the person's:

- race (including colour, nationality, descent or ethnic background)
- sex

- disability
- age
- homosexuality
- marital status
- pregnancy
- identification as a transgender person
- identification as a carer
- having HIV/AIDS.

In addition, it is inappropriate to transmit, communicate or access any material that may discriminate against, harass or vilify any person with whom you have business dealings on the grounds of political or religious conviction.

You may be individually liable if you aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. (Harassment will be treated in accordance with the grievance and dispute management policy and may result in disciplinary action).

You may not intentionally create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws. The office reserves the right to audit and remove any illegal material from its computer resources without notice.

The use of any telecommunications system to make or send fraudulent, unlawful, or abusive information, calls or messages is prohibited. Staff who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to the Deputy Ombudsman. Any staff member who initiates fraudulent, unlawful or abusive calls or messages may be subject to disciplinary action and possible criminal prosecution.

The use of a hand held mobile telephone while driving is an offence under Australian Road Rules and the office will not be responsible for the payment of any fines.

No form of computer hacking (illegally accessing other computers) is allowed.

5. Accessing certain websites

Where a genuine business reason exists that requires access to websites that would be normally regarded as inappropriate, the written authorisation of a statutory officer is required. This should be forwarded to the Security Committee.

6. Personal use

The NSW government is committed to the development of a responsive and flexible public sector and acknowledges that family and community responsibilities impact on work. In implementing flexible work practices and other relevant policies of the NSW public sector, the office recognises that its communication and information technology devices may need to be used for personal reasons. Such use should be infrequent and brief, and should not involve activities that might be questionable, controversial or offensive.

This includes gambling, accessing chat lines, transmitting inappropriate jokes, subscribing to lists, newsgroups or chat groups, sending junk programs or mail, or intentionally downloading unauthorised software or lengthy files containing picture images, and live pictures or graphics. This includes computer games, music files and the accessing of radio or television stations broadcasting via the internet. Downloading of such files increases the load on the network and could degrade the service to other staff with a genuine business need to use the internet. Personal use does not extend to the sending of non-business related written material to any political organisation.

Personal use of office communication and information technology devices is not considered private, and members of staff using such devices do not have the same personal privacy rights as they would have

when using private or public (eg. coin or card operated telephone) communication and information technology devices. Staff reasonably suspected of abusing personal use of office communication or information technology devices may be asked to explain such use (which may be monitored as part of the Ombudsman's responsibility to implement appropriate control mechanisms).

7. Record keeping

Business communications that are sent electronically (eg email messages) become official records, subject to statutory record keeping requirements. Subject to the exclusions contained in the *Ombudsman Act 1974*, they can also be subpoenaed or 'discovered' during legal processes. Business communications sent electronically must be maintained in an electronic form unless a hard copy is made and placed on an official file.

Any email sent or received in connection with a complaint or notification file should be printed and a hard copy kept on the relevant file. The electronic version is to be filed into the appropriate context folder (ie our electronic document management system) and can then be deleted from your mailbox.

You should regularly purge your inbox of superfluous emails that have been alternatively stored.

If your supervisor agrees that the bulk and relevance of email attachments is such that it would be an unreasonable use of resources to print hard copies to be attached to the relevant file, the email and attachments should be saved electronically into the appropriate context file and a notation put on the relevant hard copy file.

8. Security

Members of staff should be alert to the possibility that any messages conveyed through communication and information technology devices can be intercepted, traced or recorded by others. Although such practices are usually illegal, you should not have an expectation of privacy. Password or personal identity number protection should be used on all mobile devices (eg. mobile telephones, laptop computers, PDA's and USB drives) that are vulnerable to theft. You must take due care with all communications and the sending of confidential documents. You must exercise caution when entering into any on-line purchasing arrangements. As with telephone orders, you must first obtain proper authorisation for purchases.

Email should not be used to send Highly Protected or Protected documents unless there are special circumstances and approval of a statutory officer is given (see the Information Security Policy).

The use of your computer is monitored through a 'user id' and access rights governed by a password personal to you. Do not divulge your password to others because you could be held responsible for their actions (see the User Password Policy).

No software other than that approved by the Security Committee is to be installed on any office equipment. All requests should be submitted to help desk through a team manager.

Members of staff are not to upload any information onto any office IT equipment from a floppy disk, a CD or in any other way if virus controls are not in place.

The use of IT equipment, regardless of ownership, outside the office for the purpose of official business is subject to the following:

- personal computers should not be used at home for business activities if virus controls are not in place
- when travelling, equipment, software, computer drives, files and the like should not be left unattended in public places and portable computers should be carried as hand luggage
- when travelling, portable computers should be provided with an appropriate form of access protection, eg passwords or encryption.

You are responsible for keeping any portable computer in your possession secure. If it is stolen or lost, you must immediately report this to the Manager, IT or the Manager, Corporate.

You are responsible for keeping any office mobile telephone in your possession secure. If it is stolen or lost, you must immediately report this to the accounts section or the Manager, Corporate so that arrangements can be made for the telephone service to be suspended.

The team manager is responsible for keeping secure any office mobile telephone that has been allocated to a team for use by team members.

You must take care to maintain the security of information communicated through a mobile telephone or accessed through a portable computer, for eg, you should be careful not be overheard when having a work-related mobile telephone conversation with a colleague, and you should make sure that non-staff members cannot read what is on your computer if you are using it outside the office.

The use of and communication and information technology devices is also regulated by the NSW Ombudsman Security Policy.

9. *The office is to be accessible to the public through email*

Our internet site and other publications direct people to the general office email address nswombo@ombo.nsw.gov.au. Emails received at this address are cleared regularly. Any email obviously directed to an individual officer is forwarded to that officer electronically with a copy to the team manager. Complaints and other general email communications are sent electronically to the nominated team assessment officer.

Members of staff who have previously signed the office's policy on use of communication devices or this policy are able to receive and send external emails from their desktop.

Email may be used where that is the requested form of communication by external parties and/or where the efficiency of enquiries, investigations or other business would be facilitated by the use of email.

Email received at nswombo@ombo.nsw.gov.au will automatically be acknowledged. Emails received from external parties directly to your desktop should be acknowledged in accordance with team protocols.

10. *Complaints received by email*

It is our policy that complaints received by email are complaints within the meaning of the *Ombudsman Act 1974* and the *Community Services (Complaints, Reviews and Monitoring) Act 1993*. The *Police Act 1990* specifies that complaints received by email are complaints within the meaning of that Act. Complaints received by email must be handled in the same way as complaints received in other forms, and should be dealt with in accordance with team protocols.

11. *Form of email communications*

All email communications should conform to the same general standards of language, style and discretion as apply to written correspondence from the office. Emails should always be checked for accuracy, spelling and grammar prior to sending. An email letterhead template can be found in ADM/65. If you use this letterhead it will be necessary to insert a copy of your signature onto the template. Arrangements can be made with IT staff to have your signature scanned to enable this.

12. *Authorisation*

Any communication sent by email should be in accordance with general office procedures and your level of delegation for the signing of correspondence and any supervision approval requirements applicable. Where approval is necessary, hard copies of the approval should be kept on the file.

Any communication received by email that contains contentious material or involves a complaint about our service should be immediately brought to the attention of your team manager.

13. Clearing email while away from the office

If you are on leave or otherwise away from the office for more than three days, you must arrange to have an automated response to emails installed that advises of your absence and provides guidance on who to call if immediate assistance is required. Alternatively, you can arrange for another officer to have access to your emails, or for your emails to be automatically forwarded to another officer who will undertake to clear them by mutual agreement. Use the out of office assistant function in Outlook to do this. When returning from leave, the temporary email diversion must be disabled.

14. Dealing with CC emails

Copies of complaints sent to other agencies still need to be registered and dealt with according to existing protocols. Generally, non-police complaints of this type will be declined on the grounds of being premature and the concurrent representations.

With other cc emails, especially in cases of complainants who frequently copy to us their email correspondence to others, they should be told that such emails will be noted but will not necessarily be replied to. Action on such emails is at the discretion of the officer responsible for the matter as it would be with copied correspondence sent by ordinary mail.

15. Dealing with complainants who send excessive material electronically

A small number of complainants have been known to take full advantage of the ease of sending material electronically, including sending copies of multiple correspondence to others, photographs, reports, referrals to web sites and other material, much of it not germane to their complaints.

In circumstances where an officer forms the opinion that such communication is unreasonably diverting resources, they should discuss the matter with their supervisor with the view to getting permission to require the complainant to rationalise their communications.

However, such requirements should only be made in exceptional circumstances.

16. Breaches of this policy

Any identified use of equipment or services thought to be inconsistent with this policy or the office's Code of Conduct will be investigated. Inappropriate use may be subject to disciplinary action and a range of penalties, including termination of employment and/or criminal prosecution.

Members of staff are encouraged to report breaches of this policy to their supervisor or a statutory officer. If an alleged inappropriate use of the internet or email is notified as a protected disclosure, the matter will be dealt with in accordance with the internal reporting policy.

You should be aware that where inappropriate use is identified the Ombudsman will:

- notify the Independent Commission Against Corruption if there are reasonable grounds for believing the matter concerns corrupt conduct; and
- notify the police if it is reasonably believed a criminal offence has been committed.

OMBUDSMAN APPROVAL



Bruce Barbour
OMBUDSMAN

**NSW OMBUDSMAN
USE OF COMMUNICATION AND INFORMATION
TECHNOLOGY DEVICES POLICY**

UNDERTAKING

I have read and understand the Office of the Ombudsman policy on Use of Communication and Information Technology Devices and agree to abide by its terms.

I note that the policy constitutes the NSW Ombudsman's notice of workplace surveillance in accordance with the *Workplace Surveillance Act 2005*.

I acknowledge that the policy may be amended from time to time. I agree to read any amendment of the policy provided to me from time to time. I also agree to raise with my supervisor any concerns regarding any amendment, including if I do not understand the amendment. I agree to abide by the terms of any amendment.

Name:

Signed:

Date: