



Premier's Department
New South Wales

PROTOCOL for ACCEPTABLE USE of the INTERNET and ELECTRONIC MAIL

INTRODUCTION

The NSW Government supports wider use of developing information technology to improve the efficiency of its operations and the delivery of services to the public. This has led to a marked growth in the number of public sector workers being provided with access to the Internet and electronic mail (E-mail) as a work tool needed in the performance of their duties.

The codes of conduct in force across the public sector make it clear that all employees have a responsibility to be ethical and efficient in their official or private use (where permitted) of public property and services. This responsibility includes the use of the Internet and E-mail, both of which are services accessed from a computer terminal.

The *Employer Communication Devices Policy and Guidelines* expands on this responsibility, and encourages agencies to examine existing practices to ensure that adequate processes and procedures are in place to prevent inappropriate and/or excessive use of communication devices such as the Internet. The policy recognises:

- communication devices in NSW public sector agencies are provided for business use;
- every employee has a responsibility to be ethical and efficient in their official or private use of public property and services;
- every employee has a responsibility to be productive in the use of their work time;
- employees may need to make use of communication devices for personal purposes;
- there is a reasonable limit to which employer communication devices may be used for personal purposes; and
- employees should be provided with guidelines that clearly outline their rights on the use of communication devices.

Reasonable personal use of the Internet and E-mail should be consistent with such use of the telephone. It can include two way communication on trade union matters.

Accredited trade union delegates should be provided with reasonable access for authorised union activities.

ACCEPTABLE USE OF THE INTERNET AND E-MAIL

This protocol to the *Employer Communication Devices Policy and Guidelines* provides guidance for acceptable use by public sector employees of the Internet and E-mail and guidance on measures to be taken by Agencies. It has been developed in consultation with other agencies and the public sector unions.

Employee Responsibilities/Rights

- ❑ Computer equipped work stations and the services accessible on them are provided to employees for business use to carry out tasks related to your job. Services include the Internet and electronic mail (the applications for which include GroupWise and Lotus Notes).
- ❑ Reasonable private use of the Internet and E-mail is a privilege and such use needs to be balanced in terms of the Government's commitment to the development of a responsive and flexible public sector, and operational needs.
- ❑ Your use must be appropriate -- lawful, efficient, proper and ethical.
- ❑ Any identified use of equipment or services thought to be inconsistent with Agency policies will be investigated. Inappropriate use may be subject to disciplinary action and a range of penalties, including termination of employment and/or criminal prosecution.
- ❑ It is not acceptable to intentionally create, send or access information that could damage the Agency's reputation, 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 Agency equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.
- ❑ It is inappropriate to transmit, communicate or access any material which may discriminate against, harass or vilify colleagues or any member of the public on the grounds of
 - sex;
 - pregnancy;
 - age;
 - race (including colour), nationality, descent or ethnic background;
 - religious background;
 - marital status;
 - disability;
 - HIV/AIDS; and
 - homosexuality or transgender.

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 existing grievance and harassment procedures and may result in disciplinary action).

- ❑ You may not intentionally create, transmit, distribute, or store any offensive information, data or material that violates Australia or State regulations or laws. The Agency reserves the right to audit and remove any illegal material from its computer resources without notice.
- ❑ All information, data or files created by you while employed by the Agency are subject to scrutiny. It is important to remember that electronic messages 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.

- ❑ 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, you should not have an expectation of privacy and must take care with confidential documents.
- ❑ 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.

- ❑ Caution must be exercised when entering into on-line purchasing arrangements. As with telephone orders, proper authorisation for purchases must be first obtained. On-line purchases normally involve the use of credit or charge cards, and due regard must be had to conditions regulating their use (see the Audit Office's *Guide to Better Practice: Corporate Credit Card*).
- ❑ E-mail is not to be intentionally used for chain letters.
- ❑ Limited personal use of the Internet does not extend to intentionally downloading unauthorised software, lengthy files containing picture images, 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. Such files should not be E-mailed to others.
- ❑ No form of computer hacking (illegally accessing other computers) is allowed.
- ❑ Employees are encouraged to report breaches of this policy to their supervisor or an appropriate senior officer or executive. Internet and E-mail use should be consistent with the Agency's code of conduct, which also has guidance on reporting misuse of public resources.
- ❑ Access to the Internet should be via officially approved mechanisms only (normally through an Agency's firewall). The connection of standalone modems to individual personal computers must be authorised on a case-by-case basis.
- ❑ Where a genuine business reason exists that requires access to sites that would be normally regarded as inappropriate, the authorisation of the Agency's Chief Executive is required.

Agency Responsibilities/Rights

- ❑ The Chief Executive Officer is responsible for ensuring that access to the Internet within his/her Agency is properly controlled and monitored. The Office of Information Technology (OIT) provides guidelines on how the Internet should be used for electronic messaging. This requires adequate security protection between internal systems and the Internet.
- ❑ The Agency must provide employees with a clear statement of their responsibilities when using the Internet and E-mail. This should conform with the provisions contained in this protocol. Employees should be made aware of their role in helping to make the Agency's systems as secure as possible.

- ❑ Employees provided with access to the Internet must confirm in writing that they have read and understand the Agency's policy and guidelines on Internet and E-mail use.
- ❑ If genuine business reasons require an employee to access Internet sites that would be normally regarded as inappropriate, Chief Executives have a responsibility to ensure such access is undertaken in a suitably secure environment.
- ❑ The Agency may monitor, copy, access or disclose any information or files that are stored, processed or transmitted using agency equipment and services.
- ❑ The Agency may monitor on a random or continuous basis to:
 - prevent de-standardisation of the computer network because of the downloading of unauthorised software;
 - ensure compliance with Agency policies;
 - investigate conduct that may be illegal or adversely affect the Agency or its employees; and
 - prevent inappropriate or excessive personal use of Agency property.
- ❑ Chief Executives have a responsibility to ensure that appropriate controls and security are in place before authorising on-line purchasing. All requests and decisions relating to the authorising of such access must be documented and retained to facilitate scrutiny or audit.
- ❑ Employees must be notified the Agency will monitor Internet usage and E-mail activity to
 - ensure compliance with Agency policies;
 - investigate conduct that may be illegal or adversely affect the Agency or its employees; and
 - prevent inappropriate or excessive personal use of Agency property.
- ❑ Processes should be put in place to ensure that Internet usage and E-mail activity is adequately monitored. This should take into account:
 - the need to observe information protection principles relating to personal information (refer Data Protection Principles in the *Personnel Handbook* and the Privacy and Personal Information Protection Act 1998 – yet to be proclaimed);
 - the need to be able to link Internet sites accessed with the user identification;
 - the need to generate reports that link Internet sites with the user identification; and
 - the appointment of designated officers to review these reports.
- ❑ Procedures should be developed, in consultation with the appropriate trade unions, to determine if any inappropriate use is in breach of an Agency's normal disciplinary guidelines and whether formal disciplinary action should be taken.
- ❑ Where inappropriate use is identified, an Agency has a responsibility to:
 - notify the Independent Commission Against Corruption (ICAC) 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.

If an alleged inappropriate use of the Internet or E-mail is notified as a protected disclosure, normal procedures for protected disclosures should be followed.

- March, 1999