Department of **Consumer and Employment Protection**
Government of **Western Australia**

Our ref: WM/0443/2001
Enquiries: Andrew Harper [9222 7656]

CIRCULAR TO DEPARTMENTS AND AUTHORITIES NO. 9 OF 2002

E-MAIL, WEB BROWSING & PRIVACY POLICY UPDATE

In light of a number of issues raised within agencies, the E-mail, Web Browsing & Privacy policy has been revised.

In particular, a number of examples of prohibited activities that agencies should consider incorporating into new or existing policy, have been added.

Agencies should ensure they have an up to date e-mail and internet use policy, and that employees are well informed and understand the policy and guidelines.

Please contact your DOCEP labour relations adviser if you require further information.

JEFF RADISICH
ACTING EXECUTIVE DIRECTOR
LABOUR RELATIONS

26 June 2002

E-MAIL, WEB BROWSING & PRIVACY

E-MAIL WEB BROWSING & PRIVACY

- ***Agencies must develop policies and guidelines for e-mail and Internet usage.***
- ***Agencies must ensure that employees are aware of and understand policies and guidelines for e-mail and Internet usage.***
- ***Agencies may be vicariously liable for the actions of employees in the absence of appropriate policies and guidelines.***

ELECTRONIC MAIL

1. Electronic mail, or e-mail, is the dispatch and/or receipt of information and/or files between individuals or groups within agencies through an internal computer network, or externally through the Internet.

2. E-mail, unless encrypted, should not be regarded as secure.

3. E-mails, inclusive of attachments, are considered documents and records of the agency and are subject to agency record keeping policies.

WEB BROWSING

4. Web browsing, or Internet use, is the accessing and/or use of information or services through the Internet.

5. Internet use may include:

   a) data access;

   b) downloading of information, computer programs, graphics or sound;

   c) subscription to e-mail or newsgroup services;

   d) use of electronic 'chat' servers or programs;

   e) use of "file sharing" software;

   f) online financial transactions; and/or

   g) online gaming.

6. Internet use, and the software used to access the Internet, should not be regarded as secure.

POLICY

7. Agencies are responsible for ensuring proper e-mail and Internet use. Appropriate policies and guidelines on employee e-mail and Internet usage must be implemented to inform employees and protect the agency against any unlawful acts.

8. Agencies should consider the following aspects in establishing a policy and guidelines. The policy and guidelines should:

a) be made known to, and understood by, all staff and should be sighted by staff when logging onto the computer;

b) be expressed in plain English;

c) be explicit as to what activities are permitted;

d) be explicit as to what activities are forbidden, which may include use for:

i) the transmission and/or storage of copyrighted material;

ii) commercial activities for personal gain or profit;

iii) product advertisement or political lobbying;

iv) disclosing material, which is prohibited under state government legislation or policy;

v) accessing, distributing or storing material which could damage the reputation of the department or lead to civil liability action;

vi) false representation;

vii) solicitation of other people including other employees;

viii) providing information about, or lists of, Government employees to others;

ix) commercial solicitations of non-Departmental business;

x) activities that interfere with your job or the jobs of other employees;

xi) activities that interfere with the operation of any computer network;

xii) excessive use of the network for non-departmental business including out of hours use;

xiii) violating any law or the rights of any person or group;

xiv) accessing the service under another user name and password;

xv) communication of threatening or offensive jokes, comments or material about race, gender, age, sexual orientation, religious or political beliefs, national origin or disability; and

xvi) the use of departmental equipment to unlawfully access other networks or systems;

e) refer to appropriate additional policies and guidelines, concerning computer system security, threats and the legal liability of the agency;

f) clearly identify what information is logged or recorded and who has rights to access such records, including e-mail and browsing activities;

g) explain how staff compliance is monitored;

h) clearly express the consequences of breaching the policy and guidelines; and

i) be reviewed regularly and re-issued whenever a significant change is made.

9. Agencies are encouraged to foster an environment where employees are assured that the privacy of their communications will be respected provided there is compliance with applicable policy and guidelines.

10. It is unlikely that pervasive, systematic ongoing surveillance of staff e-mail logs or web activity should be necessary. However agencies should state that they may, but are not obligated to, monitor e-mail and Internet activity.

DISCIPLINARY ACTION

11. The policy shall clearly state that disciplinary action and/or termination could follow serious breaches of the policy.

12. Agencies should be aware when drafting policies that in cases where a serious breach occurs, the policy may be a key element of any proceedings. The policy must therefore be clear in intent and kept up to date.

LEGISLATIVE PROVISIONS

13. In the transmission or access of any material via the e-mail or internet, employees should be made aware of their responsibilities ensuring compliance with:

a) Public Sector Management Act 1994, Regulations, Code of Ethics and agency codes of conduct;

b) Equal Opportunity Act 1984;

c) Sex Discrimination Act 1984, Disability Discrimination Act 1992 and Racial Discrimination Act 1975 (Cth); and

d) other relevant Commonwealth and/or State laws such as those relating to the transmission of offensive material.