Department of the
Premier and Cabinet
Office of e-Government

Guidelines to Assist Agencies in Developing Email and Internet Use Policies

July 2004

Preface

The *Guidelines to Assist Agencies in Developing Email & Internet Use Policies* were developed in consultation with both national and local organisations. This consultation was undertaken on a draft version between June and July 2003. The feedback received has been incorporated into these Guidelines.

The guidelines are available from the Office of e-Government web site (http://www.egov.dpc.wa.gov.au) in RTF, PDF and Word formats, directly from the Policies and Guidelines section.

If you have any comments, queries or need additional information, please contact:

The Office of e-Government,
Department of Premier and Cabinet,
Locked Bag 10,
Cloisters Square,
Perth WA 6850.

Email: egov@dpc.wa.gov.au
Phone: 9213 7100

Contacts:

Sven Bluemmel
Simone Spencer

Note:

- All care has been taken to ensure that all hyperlinks provided in this document are current, accurate and in working order. However, due to the rapidly changing nature of the Internet we cannot guarantee that they will not become redundant.

Contents

Background

Context

The State Government of Western Australia (WA) supports the wider use of 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 email as a work tool.

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 use of government property and services. This responsibility also extends to the use of the Internet and email.

In the 1999/2000 Annual Compliance Report to Parliament the Commissioner for Public Sector Standards expressed concern over how the rapid growth in email and Internet use has been accompanied by misuse of e-commerce facilities. The Commissioner raised the issue that misuse by employees could affect Chief Executive Officers (CEOs) as employers, and incur legal liability for the State. In January 2002 a letter was subsequently sent to all CEOs in the Western Australian Public Sector drawing attention to this issue:

"….while your agency may have policies about the appropriate use of resources, you may wish to mention in your policy or codes of conduct appropriate warnings about:

- *Transmitting copyright, abusive, or defamatory material;*
- *Transmitting or storing material that is obscene, offensive or prohibited by law;*
- *Private commercial activities for the purpose of personal gain;*
- *Product advertisement or political lobbying;*
- *Breaching confidentiality, including the unauthorised release of departmental information;*
- *Unauthorised access and use of computers.*

Employees should be strongly reminded that email and Internet access is logged and could be monitored, and that a contravention of the policy or the code of conduct could result in disciplinary action. Employing authorities need to have systems in place to audit email and Internet use regularly. If your organisation has already provided adequate guidance to its employees, please ignore this letter. If not, you may care to review your policies and code of conduct, and draw the matter to the attention of all employees."[1]

The Government is committed to ensuring email and Internet systems are used in an appropriate manner, and that both employers and employees are aware of the issues. These *Guidelines to Assist Agencies in Developing Email and Internet Use Policies* have been issued to reinforce this commitment. They are based on established and recognised guidelines developed by a selection of WA Government agencies, other states and territories as well as international jurisdictions and sources.

[1] Letter to all CEO's from Don Saunders, Commissioner For Public Sector Standards, 14 January 2002.

How can the Office of e-Government Help?

Whilst these Guidelines have been developed for agencies to use as a tool when developing their own email and Internet use policies, the Office of e-Government is available to provide further assistance if agencies require.
The Office would also appreciate feedback from agencies regarding their experiences in developing email and Internet use policies and on any issues that should be included in future versions of these guidelines.

Purpose

The purpose of these Guidelines is to provide assistance to agencies wishing to develop their own email and Internet use policies. A sample policy from the Department of the Premier and Cabinet has been included at the beginning of these Guidelines to provide agencies with a working example of what an email and Internet Use Policy may contain.

In addition to this sample policy, these Guidelines provide a summary of potential content areas that agencies may wish consider when constructing their email and Internet use policies or when reviewing any existing policies they may have.

It is important to note that the examples outlined in these Guidelines are provided as a reference point for agencies and that it is up to the individual agency to decide the nature and content of any email and Internet use policies they may wish to develop.

It is not the intention of the Guidelines to be definitive. They are intended for use as a tool to assist in the development of email and Internet policies. Although many of the issues that surround Internet and email use will be the same in all agencies, such as security and records keeping requirements, there may be procedural and process issues that will be specific to individual agencies. There is a clear need for flexibility and variation in practices across agencies. Agencies may choose to develop an overall policy for this area, or may select to develop discrete polices for email and Internet use. Some agencies may want to be very prescriptive, not permitting personal use for example, while others may want to be more flexible and allow either limited or unlimited personal use.

As per the Commissioner for Public Sector Standard's recommendation, the most critical issue is that agencies at least have some form of policy or policies defining the parameters of email and Internet use in their organisation.

This document provides the resources that will allow the development of email and Internet use policies that better reflect the needs of individual government organisations. Therefore, these Guidelines should be viewed as a menu of issues that can be considered for inclusion in any agency's policy.

Guidelines

Sample Policy

Department of the Premier and Cabinet
Computing and Communications Acceptable Use

Policy

The Department encourages its officers to enhance customer services, productivity and increase knowledge through the use of available computing and electronic communications facilities, including the use of the Internet, within the bounds of their employment, and legal and ethical conduct requirements.

The policy is intended to cover Department staff use of the following facilities:

- All computer hardware, network and communications equipment
- All computer software and applications, including all Internet applications
- Telephones and fax machines

Guidelines

Use of any Department computing or communication resources by an officer should be restricted to employment related purposes and all associated behaviour must be in keeping with the Code of Ethics as prepared by the Public Sector Standard Commissioner and the Laws as they apply to all residents of the State of Western Australia.

Limited personal use of facilities by staff is also permitted provided:

(i) It is endorsed by local management
(ii) It does not interfere with work, or the work of anyone else and
(iii It does not involve unethical behaviour

Common sense should dictate what is and is not employment related, and also what constitutes illegal and unethical behaviour in this regard. Notwithstanding this however, the following are specifically prohibited:

- Private commercial activities for the purpose of personal gain.
- Accessing, distributing or disclosing material prohibited by policy or law
- Breaching confidentiality.
- Unauthorised copy or transmission of copyrighted material
- Transmitting threatening, abusive, defamatory or offensive material
- Distributing chain letters.
- False representation.
- Unauthorised use or release of Department information.
- Unauthorised access to and use of computers.

Responsibilities

When using government computing and communications resources and facilities, officers are expected to be aware of their responsibilities to:

- Comply with all legal, legislative and administrative requirements.
- Ensure any action taken serves to enhance the services provided by the Department, and not bring the Department into disrepute.
- Be informed of all security requirements related to the use of computer facilities, and in particular the security risks involved in using the Internet and ensure that this is not compromised by their actions.
- Seek advice if they are unsure about the status of their actions.

Officers who knowingly breach this policy may be dealt with under the disciplinary provisions of the Public Sector Management Act or the provisions of any other relevant statute.

While it is the individual officer's responsibility to use resources appropriately, management also has a responsibility to deal with both deliberate and inadvertent breaches of the policy.

Storage of Information and Monitoring of Use

Staff are advised that all information, stored on Department Network Servers is backed up nightly. Similarly detailed statistics on usage of the telephone systems and the Internet are automatically logged and records kept on backup tapes.

Monthly backup tapes are kept for several years.

Systems are backed up primarily for disaster recovery purposes. However on instructions from the Director General or as a result of Inquiries, Investigations or Freedom of Information requests this information may be scrutinised or made public.

Systems are also routinely monitored by IT staff to ensure satisfactory levels of service. Monitoring may also be carried out at the instruction of the Director General. Instances of blatant abuse of this policy are required to be reported to local management or the Director General.

Policy Content Guide

This section includes content areas that can be incorporated into the actual policy document. Again it should be stressed that this is not a definitive listing but rather a guide, as some agencies may want to include more or less issues or detail in their policies. This section also looks at some of the process (decision) issues that surround the specific areas or topics.

Policy document contents suggested for email and Internet use policy is outlined as follows:

1. Purpose and Scope
2. Objectives
3. Procedural Issues
4. Security
5. Privacy
6. Legal Requirements
7. Acceptable and Prohibited Use
8. Acknowledgement of Obligations
9. Monitoring
10. Breaches and Consequences

Purpose and Scope

Purpose

The purpose of the policy should be clearly described including the reasons why it should be read and understood. For example:

1. "The purpose of this policy is to ensure that all users of the *Name of Agency* email service are aware of the conditions concerning its use as a means of correspondence with both internal and external parties".

2. "The purpose of this policy is to ensure that all users are aware of the *Name of Agency* conditions concerning the connection to and use of the Internet services via *Name of Agency* information resources."

3. "The purpose of this Internet Acceptable Use Policy is threefold:

    a) Document what is and is not acceptable use of the Internet during organisation time and/or over the organisation's network.
    b) Protect the organisation against potential liabilities.
    c) Promote awareness of the benefits and risks of Internet use."[2]

Scope

The scope should explicitly state who and what is governed by the policy. For example:

1. "This document details the email and Internet acceptable use policies to be followed by the *Name of Agency* employees. All levels of management are required to actively support its implementation."

2. "This policy applies to all staff, contractors and consultants employed by *Name of Agency* who use the *Name of Agency* email and Internet services. It covers the use of email by government employees including:

    a) Internal use of email.
    b) Remote use of email.
    c) Email sent and received via external networks such as the Internet.
    d) The procedures required to ensure that Internet practices comply with agency requirements and to ensure that the benefits of using the Internet are maximised for the agency".

3. "From the *Name of Agency* point of view, the Internet is like any other form of communication. Staff have the same privileges on the network as they have now with the telephone, fax, and keyboard, but they also have the same responsibilities. Contact with other people and organisations must be made on that basis."

[2] Internet Acceptable Use Policy Guidelines from Vicomsoft. http://www.content-filtering.com/acceptable_use_guide.html

4. “The standards of acceptable use prescribed in this policy apply to every user, regardless of the technical method, location and or access means by which that user has connected to the network.”

Reference should also be made to any other relevant policies, such as the Information Security Policy, Code of Conduct, etc. If the policy replaces an existing policy this should also be stated.

Objectives

The objectives of the policy should be clearly defined. Objectives may include to:

1. "Increase understanding of the requirements for the use and management of email, the Internet and Intranet in *Name of Agency*."

2. "Reduce corporate exposure from inappropriate email and Internet practices and to ensure compliance with legal requirements such as freedom of information requirements and the State Records Act, 2000."

3. "Increase understanding by employees that their actions may have legal implications and could adversely affect them, if they act outside the policy/guidelines."

4. "Promote acceptable use of email and the Internet in the agency thereby resulting in benefits such as:

    a) Enhanced customer services
    b) Improved ability to store and recover critical information
    c) Reduced corporate risk from inappropriate email and Internet practices"

6. "The use of *Name of Agency* computing and communication resources imposes certain responsibilities and obligations on all personnel employed by or contracted to the *Name of Agency* and is subject to the provisions of the Public Sector Management Act 1994 and the Western Australian Public Sector Code of Ethics published by the Public Sector Standards Commission. The objective of this policy is to ensure that Internet use by personnel abides by these and all other relevant codes, laws and guidelines."

Procedures

The procedures for the use of departmental information technology systems should be detailed. Examples of content that may be relevant for use under the heading of 'procedural issues' include:

Access

The agency may grant access to all employees or it may provide access on a more selective basis. It may be granted in an open or a more prescriptive fashion. This will determine the type of information the policy provides. Content that may be used, for example is:

1. "The granting of access is to be subject to the person's understanding of, and agreement to, comply with current policies and relevant procedures concerning the use of the Internet services. All staff using the *Name of Agency* network have access to the Internet and email and the ability to copy material and save it to disk ('downloading'). Access is work-related. Staff can use this access for departmental business or for professional development, but are not authorised to use it for other business or for personal financial gain."

2. "The granting of access to the Internet and email is to be authorised by the appropriate director or manager who will take into account the person's needs or the benefit of such access. Access requirements will be reassessed where the person's job description or role changes."

3. "After a staff member or contractor has completed induction, an email account will be assigned. The electronic mailbox must be operated in accordance with this policy. The content, maintenance and use of an electronic mailbox are the responsibility of the person to whom the email account is assigned."

Email Specific Procedures

1. Sending and Receiving Email

The requirements for sending and receiving email can be included. These may cover a number of areas. Examples include:

a) Sending email to broadcast groups, e.g. "Sending email to broadcast groups (e.g. *All Agency Name*) is to be used with discretion. An alternative method, like the Intranet maybe more appropriate for some information."

b) Email sent to multiple external recipients, e.g. "Email sent to multiple external recipients (e.g. Newsletters) must be addressed using the Bcc (Blind Copy) address block unless the privacy of recipients is not a consideration (e.g. members of a working group)."

c) Notices, e.g. "All email messages sent through the departmental system contain a standard disclaimer/legal notice."

d) Confidentiality, e.g. "If staff are sending a confidential message, it is necessary to mark the item as such."

e) Distribution level, e.g. "If the item is not for further distribution (other than the intended recipient) and is subject to copyright considerations, it is the responsibility of the sender to clearly indicate this in the email."

f) Records e.g. "Emails related to the agency's business activities are state records and must be captured in the corporate records system".

2. Email Formats

This section may also provide the opportunity to reinforce to staff that email is a communications mechanism and should be made as accessible and usable for users as possible. The *Guidelines for State Government Web Sites*[3] deal with this issue in more detail and state: "Avoid using html formats or, offer users the choice of requesting the format most suitable for them. There are usability problems for customers with html only format as not everyone has the capability, the bandwidth or desire to access html e-mails". An example of content that can be used for this issue is:

"Good format for electronic mail communications is:

a) Messages transmitted as 'text' or 'rich text'.
b) Text in either Arial or Times New Roman font for the body of the message.
c) Messages that are not transmitted as 'html'.
d) Do not contain additional graphic images that are not essential to the purpose of the message.
e) Do not use fonts that are not easy to read on the screen."

3. Response Policy

Email is a 24x7 form of communication. People use email with the expectation of receiving a timely response - emails should therefore be responded to in a timely manner. An example of policy content for email response time is:
"A response should be sent to the sender of an email within at least one working day of receipt of the mail."
Please note that this timeframe is an example only and you may wish to set a response timeframe that is more suitable to your agency's core business.

4. Arrangements for Leave

Given that people use email with the expectation of receiving a timely response, arrangements should be made for email when a staff member takes leave. An example of policy for this issue is:

"Staff taking leave must ensure that, in their absence, their mail-boxes are set up to:

a) Ensure that all incoming emails are considered during their leave.

[3] http://www.egov.dpc.wa.gov.au/index.cfm?fuseaction=projects.policy

b) Provide automated replies to senders advising of their absence and providing email, fax and telephone contact details of the person undertaking duties while they are away.

c) Remove themselves if possible from broadcast groups or list servers prior to taking leave.

d) Staff taking leave should consider allowing proxy email access to another staff member. Automated replies should be removed as soon as staff resume their duties".

5. SPAM

Spam is the common term for unsolicited bulk electronic messages, usually electronic mail messages but increasingly SMS and MMS messages (text messages and graphics/videos delivered to mobile phones). These messages are typically sent to a large number of recipients who have not requested them. It is fairly easy and cheap for spammers to send large amounts of unsolicited mail – the cost is borne by recipients in download costs and time spent sorting through rubbish mail in order to find their regular personal and business mail. Some people are deluged with hundreds of spam mails every day.

It may be worth including in the policy the procedures or processes that staff can take to minimise the amount of spam they are exposed to and/or the reporting mechanisms required to notify the relevant area responsible for blocking spam.[4]

Internet Specific Procedures

A down side to the Internet's exponential growth of new users and services is the enormous demands on network capacity and bandwidth availability. Abuse of the Internet impacts its capacity, efficiency and future viability. Employees should therefore be aware of unethical and unacceptable activities which purposely:

1. Seek unauthorised access to Internet resources.
2. Disrupt the intended use of the Internet.
3. Waste Internet resources (people, capacity, computers) through disruptive actions.
4. Destroy or threaten the integrity of Internet information.
5. Compromise the privacy of users.

It should be made clear that agency-provided Internet privileges, like computer systems and networks, are agency resources intended to assist in the fulfilment of duties. It may be appropriate to explain to staff that communications facilities at work are there for the business purposes of the employer and employees are expected to behave responsibly when using communications facilities at work.

[4] See the Department of Communications, Information Technology and the Arts site for more information
http://www2.dcita.gov.au/ie/trust/improving/spam

Internet Use Issues

Requirements that need to be taken into account by staff when using the Internet can be discussed in the policy and may include the following:

1. **Subscription to Lists**

   For example: "Subscription to list servers is to be kept to those that relate to the agency's activities - subscription to lists that are not work related is not permitted. In order to ensure a manageable level of emails received, which will not interfere with normal working obligations, it is advisable to limit the amount of lists to which you subscribe.

2. **Restriction on Sites that can be Visited**

   For example: "The *Name of Agency* may monitor usage of the Internet by employees, including reviewing a list of web sites accessed by an individual. No individual should have any expectation of privacy in terms of their usage of the Internet. In addition, the *Name of Agency* will restrict access to certain sites that it deems are not necessary for work related purposes. These include sites that contain illegal, obscene, pornographic or hateful content, which is objectionable or inappropriate in the workplace."

3. **Downloading**

   For example: "Software should not be downloaded from the Internet without prior approval of the IT Department. Downloaded software can introduce computer viruses onto the *Name of Agency*'s network. In addition, anti-virus download software is not to be disabled. All computers are configured to automatically scan any material downloaded from the Internet."

4. **Fees for Online Information**

   For example: "The Internet provides access to many sites that charge a subscription or usage fee to access and use the information on the site. If costs are appropriately incurred on behalf of the *Name of Agency*, the user may submit the charges for reimbursement on expense reports, subject to customary review by the Finance Department. All items that are charged to the *Name of Agency* are subject to the same approval process as other business-related expenses. Requests for approval should be submitted to the appropriate manager."

Other Issues

Where technical restrictions on agency email and Internet are in place, such as email size, downloads from the Internet, attachments and mailbox limitations, these should be explicitly stated in the policy. Examples of policy in this area include:

1. **Content of Mailboxes**

For example: “Mailbox contents are electronically restricted to a maximum of 1000 messages. If the contents exceed 1000 messages, the email facility will no longer be available. Functionality will be restored when the number of messages is reduced to below 1000”.

2. Attachments

For Example: “To ensure optimal use of email capacity, attachments that are multimedia based, programs or larger than 2MB are blocked by default. Contact IT when you have a business requirement to send or receive such attachments. Distribution of attachments to a large number of people should generally be avoided. It is recommended that attachments should be:

a) Placed on the Internet and referenced by a hyperlink in the email
b) Scheduled to run after business hours.
c) Approved by IT support before distribution”.

“The Internet connection is a shared resource. While routine email and file transfer activities do not affect service levels significantly, large file transfers and intensive multimedia activities will impact the service levels of other users. Users contemplating file transfers over 10MB per transfer, or interactive video activities, should schedule these activities after business hours, or early or late in the day.”

3. Passwords

For example: “The use of your computer, email and the Internet 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.”

4. Encrypting email

For example: “Employees may encrypt their email and files only with approved software. *Name of Agency* may require a copy of any key necessary to access encrypted email messages or files as well as a copy of any password used.”

5. Downloads and Viruses

For example “Employees may not use email systems to download software.” *Or “* Employees may not use email systems to download software unless it has been checked with appropriate virus software to ensure it is virus free.”

6. Signature blocks.

A signature block is a short, usually text, block of information inserted at the close of an email message. Depending on the email program used, it could be a separate file, or stored within the program itself. To help ensure a consistent public image is generated, it is recommended that agencies utilise a consistent approach to signature blocks. Where online services are provided by the agency it is recommended that links/URL’s to these services should be provided in the signature block. For example content of a signature block can include some of the following information:

a) Name.
b) Position and/or Team.
c) Department.
d) Full postal address.
e) Phone.
f) URL of the web site.

Staff should be made aware of any technical restrictions in place and of their resulting obligations.

Security

Security Issues

There are three main classes of threat presented by the Internet:

1. Connection to the Internet provides a pathway into the IT system. This pathway provides a route for 'hackers'. The threat posed by viruses in message attachments is equally significant.

2. Internet traffic may pass through nodes in many different places. It is possible for a node to scan traffic and copy interesting messages, i.e. confidentiality is not assured. However, in reality the risk of this is probably very low, with the exception of where an 'attractive' agency can be specifically targeted at a node that handles much of its traffic. In this case encryption may need to be considered.

3. 'Spoofing', is a problem of message authenticity. It is where someone sends a message purporting to be from someone else. It is very easy to achieve this on the Internet. Users should be aware of the possibility of it happening.[5]

In order to address a wide range of security issues, most agencies have put security policies in place. It is recommended that such security policy should be considered and reference made to it in email and Internet use policies. Issues that you may wish to specifically make staff aware of in regards email and Internet use include:

1. The sending of large attachments with emails, the transmission of chain letters or mass mailing (spam), or the down-loading of data or programs, which may place unnecessary strain on system resources.

2. The potential of downloaded software/files and attachments in email to introduce viruses. Firewalls may not protect networks from viruses - downloads and attachments need to be scanned prior to use.

3. Security arrangements such as access control, passwords, etc.

4. If used - encryption methods, digital signatures, PGP, etc.

5. Ensuring that all breaches are to be reported to the Internet Administrator or to the IT Security Officer immediately when discovered.

Examples of **content** that support security and may be included in the email and Internet Use policy are:

[5] For more in-depth information on security risks and issues see the GOVSECURE website: http://agate.gem.wa.gov.au/prod/wa/govsecure/public/home_page.html

Example One

"Name of Agency has adequate security arrangements in place to protect the network from unauthorised access. Employees are required to support these security arrangements:

1. Access to the Internet should be via officially approved mechanisms only (normally through the firewall). The connection of stand-alone modems to individual personal computers must be authorised on a case-by-case basis.

2. Where external access is to be provided, security controls will be established to ensure no alternative path to the Internet services can be gained from *Name of Agency* applications. No exceptions or entry points will be allowed.

3. Allowing other employees to use or access email accounts unless authorised by management is not permitted.

4. When there is suspicion of a virus staff must note the symptoms and any error messages appearing on the screen, isolate the workstation if possible, inform IT immediately and not attempt to transfer information to another computer."

Example Two

1. The transmission of confidential or commercially sensitive information over the Internet is not permitted, except where that information is encrypted using a technique covered by a *Name of Agency* standard.

2. Users are obliged to report to their Local Security Officer any security incidents or vulnerabilities of which they become aware.

3. A user must not advise anyone of his or her password, nor allow it to be accessible by anyone.

4. A user must not at any stage leave a device unsecured whilst logged on with their personal logon-id.

Privacy

There are several aspects with regard to privacy in this arena:

1. Access controls and security features of a network (passwords etc.) give the user an illusion of privacy and they may not be aware that their browsing activities and email content can be scrutinised.

2. Privacy on the Internet has two distinct aspects:

    a) Concerns with information published to a web site.

    b) Concerns with information that is collected via a web site, such as for a newsletter or mailing list and through the use of cookies.

For the purposes of these guidelines, information published to a web site will be discussed in more detail.[6]

Issues

While there is strictly speaking no 'right' to privacy in common law, employees do have the expectation of being treated with decency and dignity at work. These 'rights' include being left alone; quiet enjoyment of their work; not having personal matters disclosed; and tolerable working conditions. Email and Internet monitoring may cut across those rights.

However, employers have rights as well - to protect property and persons; monitor employees' performance; improve customer service; protect against false workers compensation claims; promote occupational health and safety; monitor production; and staff training and development.

Getting the balance right requires thought.

Regulation

In December 2000, the Federal Government, under the Privacy Act 1988, introduced "light touch" privacy legislation, the National Privacy Principles (NPPs) to cover the private sector.

The Information Privacy Principles (IPPs) under the Commonwealth Privacy Act 1988 apply to Commonwealth and ACT Government agencies. The Western Australian Government is not yet governed by any legalisation in this area. However, the Department of Justice is currently working on new laws that will ensure electronic information systems are not abused. It is expected that this new legislation will to be passed in 2004. In the interim, it is advisable to utilise privacy best practice principles and in particular, the IPPs used by the Commonwealth and ACT Governments.[7]

[6] For guidance on information that is collected via a web site, see the *Guidelines for State Government Web Sites* - http://www.egov.dpc.wa.gov.au/index.cfm?fuseaction=projects.pprocedures

[7] See http://www.privacy.gov.au/government/index.html for more information.

Privacy and Email

It is recommended that the agency email policy should make it clear to staff that as the agency has responsibility for its computer systems and networks, it has the right to make directions as to its use.

Informing people about the personal information that is collected and held, and what is done with it, is an important privacy principle. It is encouraged as best practice that agencies develop (in consultation with staff) a clear privacy policy in relation to staff use of computer networks, particularly with regard to the use of email. Balancing the legitimate interests of organisations and staff may be difficult and this balance may vary in different organisations. It is important to note that policy or practice that lead staff to believe that their privacy in the workplace is not respected may be regarded as intrusive and oppressive and have a negative impact on morale and productivity.

For more detailed information on this issue see the Privacy Commissioners Guidelines for Workplace Email, Web Browsing and Privacy. The following examples can be incorporated into the email policy:

Example One

"All email messages on the departmental system are automatically logged and are subject to scrutiny by system administrators and auditors. The CEO, or staff specifically authorised by the CEO, may review, copy or delete any email messages and may disclose messages to others. Messages conveyed by email are capable of being intercepted, traced or recorded by others. You should not have an expectation of privacy and must take care with confidential documents."

Example Two

"The organisation provides email to assist in conducting business; therefore emails are company property and can be traced if necessary (even if messages have been deleted). The content of electronic communications is not the personal property of the employee. Like other forms of text-based communication, email is the property of the employer and will be treated as such."

Example Three

"Policy: *Name of Agency* does not guarantee the confidentiality or privacy of information within electronic communications.

Implementation Guidelines:

1. Staff must not send confidential or sensitive information via electronic mail.

2. The following disclaimer is automatically attached to all electronic mail messages transmitted outside *Name of Agency* Facilities:

   The information contained in this e-mail may be private and personal or otherwise confidential. If you are not the intended recipient, any use, disclosure or copying of

any part of the information is unauthorised. If you have received this e-mail in error, please inform the sender and delete the document."

Privacy and the Internet

Most web sites are accessible to anyone with web access. Most sites provide information and/or publications. The information and publications may contain information that can raise privacy concerns. Agencies should carefully consider the appropriateness of:

1. Placing information and publications that contain personal information on the web, as this information may be exposed to a much wider audience than originally intended.

2. Publishing on the web, personal information that was collected for inclusion in a less widely available publication.

Staff should be made aware that if their personal information is published on the web, it will be accessible to millions of users, that their information can be searched for using an identifier such as the individual's name and that their information can be copied, and used by any web user. Most importantly, staff should be made aware that once their personal information has been published on the web, the agency has no control over its subsequent use and disclosure.

Government staff are entitled to the same protection as government clients. All staff members should be advised if their personal information is to be published on the web. The publication and easy accessibility of this information may place staff at risk of receiving unsolicited e-mail (spam) and unwelcome attention from a range of people and organisations. The publication of information such as staff classifications may make the information even more interesting to third parties as the salary range associated with these classifications is publicly available information.

There may also be danger to particular staff in publishing their personal information on the web. Individuals may be placed at risk of harassment particularly if their work involves contact with members of the public. For personal safety reasons individuals may not wish that their work contact details be published.

There may also be instances where personal information is incidentally or accidentally published on the web, for example personal information may be included in documents which are then published on the web. It is recommended that documents be carefully checked before being published on the web and any unnecessary personal information removed or that consent to publish the information is obtained from the individual concerned.

For more in-depth information and guidance on this issue, it is recommended that the Office of the Federal Privacy Commissioner's Guidelines for Federal and ACT Government Website be consulted.

Where agencies collect information from clients via the web site, including for example through forms, online transactions, newsletters, etc., this should be done by sufficiently secure means. Individuals also should be provided with alternative means of providing personal information to the agency, other than via the web site. The Privacy statement should address security issues where appropriate. See the Guidelines for State Government Web Sites for more information on this issue

Legal Requirements

Relevant Legislation

The email and Internet use policy should refer to relevant legislation. Government policy in Western Australia in this area is governed by, but not limited to the following:

- State Records Act (2000)
- Copyright Amendment (Digital Agenda) Act (2000)
- Public Service Regulations (1998)
- Evidence Act (1996)
- Public Sector Management Act (1994)
- Freedom of Information Act (1992)
- Financial Administration and Audit Act (1985)
- Copyright Act (1968)
- Library Board of Western Australia Act (1951) (Sections 22 - 30)
- Limitation Act (1935)
- The Criminal Code (Section 85)
- State Records Office's Records Management Policies and Standards Manual
- Public Sector Code of Ethics

Relevant agency policies should also be listed, such as the Information Security Policy, Code of Conduct, etc. Some areas that may need to be discussed in the policy in more depth are listed below.

Copyright Issues[8]

Material in electronic form, such as on the Internet or in email may be protected by copyright. However, many people publish material on the Internet and give permission for people to copy it for certain purposes. Similarly, an email and its attachments may be protected. In some cases the sender may have given an implied permission for the email to be forwarded or printed.

The Commonwealth Copyright Act 1968 regulates copyright in Australia. Copyright protects a range of material including:

- Written material (such as novels, song lyrics, Reports, newspaper articles and **emails**);
- Musical works
- Computer programs
- Films
- Artistic works
- Images
- Dramatic works
- Compilations
- Sound recordings

[8] Australian Copyright Council Online Information Centre http://www.copyright.org.au

Copyright and Email

Copyright protection for email is not new, as text is generally protected by copyright. Copyright owners have a number of rights, including the right to control the reproduction of their material and the right to control the communication of that material to the public. Generally, copyright will be infringed where the copyrighted material is used without permission in one of the ways that the copyright owner controls or in circumstances to which no exception applies.

Copyright issues arise when an email is forwarded, as a reproduction is likely to be made on the recipient's computer. Where emails are distributed in a business or educational context (or any context other than between family and friends), the communication may also constitute a "communication to the public".

However, in many situations, there will be an implied permission from the copyright owner to forward an email. For example, in the context of a government department, a permission to forward an email, onto relevant people in the organisation (such as administrative staff and the people who might be expected to deal with the email) would generally be easy to imply. On the other hand, it may be very difficult to imply permission to forward an email to people who would not be expected to receive or deal with it, or to post it to a web site. The email policy should make staff aware of this.

Copyright is a large and complex issue and it is outside the scope of these guidelines to deal with the issue in great detail. However, it is one that needs to be considered when developing an email policy. For more in-depth information on copyright and how it may affect the use of email and the Internet, visit the Australian Copyright Council Online Information Centre[9] or talk to the Crown Solicitors Office, Phone: (08) 9264 1888.

Copyright and the Internet

Copyright and the Internet is increasingly becoming an area where caution needs to be exercised. It may be relevant to inform employees of their obligations and the related issues. It is beyond the scope of these Guidelines to discuss copyright in detail but more information can be found in the Australian Copyright Council's - *Information sheet G56 Internet: Copying from March 2001* available from the Councils Online Information Centre[10]. Advice can also be sought from the Crown Solicitor's Office. However, it is clear that downloading or disseminating copyrighted material that is available on the Internet maybe an infringement of copyright law. The downloading or posting of any copyrighted material from any source to an agencies network may also be an infringement of copyright law. Permission to copy the material must be obtained from the publisher.

An **example** of how one agency has dealt with the issue in their Internet policy is as follows:

"Published material is usually protected by copyright unless the copyright owner expressly gives permission for others to use it. Staff who copy material from the Internet must use it discreetly, not borrowing from it publicly without acknowledging the source (author, title, publisher, Internet address) where known. As for this agency, the Department's Internet home page, is linked to a Copyright and Disclaimer page, which carries a message similar to this: © *Name of Agency*, 2003. The Department claims copyright on the information at

[9] http://www.copyright.org.au
[10] http://www.copyright.org.au

this site unless the copyright of others is acknowledged *in situ*. The information is provided as a service to the community. It is made available in good faith and is derived from sources believed to be reliable and accurate. Nevertheless, the authors of this site expressly disclaim liability for any act or omission done in reliance on that information or for any consequences of them."[11]

Record Keeping Issues

Government agencies should be aware that they need to create and manage electronic records with the same care as they manage paper records. All digital data created or received in the conduct of government business are defined as records under the State Records Act 2000 *(WA.)*[12]

The Act defines electronic records as those: *"communicated and maintained by means of electronic equipment…electronic records include…electronic mail and electronic messages, Internet and Intranet systems…"*

A number of policies and standards published in *'The State Records Office Policies and Standards Manual*[13]*'* are applicable to the management of electronic records. The most appropriate is State Records ***Policy No 8****: "Policy for the ongoing management of electronic records designated as having archival value"*. This policy "…is provided to ensure that public records in electronic format, having been assessed as being of archival value, are preserved and accessible for as long as they are required"…

As well as Policy No: 8, the State Records Office has released three *State Records Standards* - Numbers 4, 5 and 6, in relation to electronic/online records:

1. **State Records Standard 4**: *Records Management Standard for the Management of Electronic Mail (E-Mail).* This standard was developed to provide best practice guidelines for the management of records created or received in email applications by state or local government agencies. Focussing primarily on the role of the record-keeper with regard to the capture of email, the document covers topics such as security requirements, admissibility as evidence, digital and electronic signatures, registration within an agency's record-keeping system, and email naming conventions.

2. **State Records Standard 5:** *Standard for the Management of Electronic Documents in Networked Computer Environments.*

3. **State Records Standard 6:** *Standard for the Management of Electronic Documents in Stand-alone Computer Environments.*

Web sites created by an agency are also state records and are subject to the same record keeping requirements as state records in other formats. In order to assist agencies to deal with State Records compliance, the Guidelines for the Management of Web Information (as per the State Records Act, 2000)[14] have been developed by a cross-government team[15].

---

[11] The Internet and the CALM Web - Information and Guidelines. The Department of Conversation and Land Management.

[12] A selection of relevant links for State Records: http://www.slp.wa.gov.au/statutes/swans.nsf/be0189448e381736482567bd0008c67c/3988e10065ed24a948256a5d0004cf94?OpenDocument and http://www.sro.wa.gov.au/about/sra2000.html

[13] http://www.sro.wa.gov.au/src/policies.html

[14] http://www.indtech.wa.gov.au/govt/polguides/websites/webinfo.htm

This information paper has been designed to assist government agencies address some of the practical issues associated with managing web based information that have arisen as a result of the State Records Act 2000.

Working with the agency's record-keeping staff is extremely important in ensuring that email and Internet use policies comply with regulations as per the State Records Act. To purchase a copy of the State Records Office Policies and Standards Manual, or for general advice and guidance contact the State Records Office[16] on (08) 9427 3365.

An **example** of content included in one agency's policy is:

"In using the *Name of Agency* computing and communication facilities, normal records management and archiving practices must be adhered to as follows:

1. All correspondence produced or received by an officer in the course of their duties are deemed to be state records.
2. Records created or received electronically are subject to the same conditions as paper based records.
3. It is the responsibility of the individual officer to ensure all documents relating to the business operations of the *Name of Agency* are forwarded to records management for recording."

Disclaimer Issues

The most commonly used risk management tool in the online environment is the disclaimer. A disclaimer is a written statement that attempts to avoid or disclaim liability that could otherwise arise by operation of law. For disclaimers to be effective, the words used:

1. Must be clear (the courts have been quick to find ambiguities in disclaimers and interpret them narrowly).

2. Have been brought to the attention of the individual concerned prior to that person engaging in the conduct the disclaimer is expressed to cover.

Email disclaimers are statements that are mostly included at the bottom of an email. These statements are usually of a legal character (for example, they can be used to detail the copyright of the material) but can also be used for marketing purposes. If the agency utilises an email disclaimer, it must ensure that staff are aware of the contents of the disclaimer. A web site disclaimer is usually included in the footer of every web page and often includes terms and conditions of use as well as disclaimer information.

Why use a disclaimer?

If the agency was unlucky enough to be sued for the contents of an email, it is not clear whether or not an email disclaimer would protect it from liability in a court of law. In fact, it is not clear if disclaimers are worth the 'virtual paper' they are written on, as they are often difficult to enforce. However, it may help your case and it is probably better to have one than not. The use of disclaimers is therefore recommended. Some examples of disclaimers are:

---

[15] The Department of Agriculture; State Records Office; Department of Justice; Department of Premier and Cabinet; and the Department of Industry and Resources.
[16] http://www.sro.wa.gov.au/

Example One – Email

"The *Name of Agency* Legal Notice. The contents of this email or its attachments may be private and confidential and may be privileged or otherwise protected from disclosure in the public interest. If you are not the intended recipient of this email please notify the sender, delete the email and attachments from your system and destroy any copies you have taken of the email and attachments. Before taking any action based upon advice and/or information contained in this email you should carefully consider the advice and information and consider obtaining relevant independent advice".

Example Two – Web site[17]

"The *Name of Agency* makes this material available on the understanding that users exercise their own skill and care with respect to its use. Before relying on the material in any important matter, users should carefully evaluate the accuracy, completeness and relevance of the information for their purposes and should obtain appropriate professional advice relevant to their particular circumstances. The material at this site may include views or recommendations of third parties, which do not necessarily reflect the views of the *Name of Agency* or the State of Western Australia or indicate its commitment to a particular course of action. By accessing information at or through this site each user waives and releases the *Name of Agency* and the State of Western Australia and its servants to the full extent permitted by law from any and all claims relating to the usage of the material made available through the web site. In no event shall the *Name of Agency* or the State of Western Australia be liable for any incident or consequential damages resulting from use of the material.

[17] For more information on the legal issues associated with online services, please see the Guidelines for State Government Web Sites – Section 9
http://www.egov.dpc.wa.gov.au/index.cfm?fuseaction=guidelines.legal

Acceptable and Prohibited Use

Each individual agency should determine what is 'appropriate use' of its computer systems and networks. It needs to be absolutely clear to staff what is and is not acceptable use – it should be explicit.

Email Acceptable and Prohibited Use

Details of email activities that are specifically prohibited should be unambiguously stated. Examples are:

Example One

"Use of email throughout the agency network infrastructure is permitted where such use is required for business purposes, effective internal/external communications and supports the goals and objectives of the agency and its business units. Employees shall act, when using email, in an ethical and professional manner, consistent with the *Name of Agency* Code of Conduct. Staff must ensure the department's email is not used for:

1. Illegal or unethical purposes.
2. Distributing threatening, abusive, defamatory, prohibited or offensive messages.
3. The practice of harassment, abuse or defamation of any person.
4. Distributing chain letters, SPAM or unnecessary multiple messages.
5. Making false representation or breaching confidentiality.
6. Accessing, distributing or disclosing material prohibited by policy or law.
7. An activity designed to deny the availability of electronic communications.
8. Unauthorised copying or communications of copyrighted material.
9. Unauthorised use or release of agency information.
10. Providing employee information to any non-authorised third party.
11. The distributing and/or knowingly receiving of unauthorised software.
12. Potentially embarrassing or negative impacts on the Department.
13. Private commercial activities or for the purpose of personal gain including selling or promoting goods or soliciting business of any kind.
14. Unauthorised destruction of corporate records.

Ephemeral emails referring to non-business matters (e.g. social events, footy tipping) should be utilised on a limited basis. These should be discarded after use to ensure system and network resources are not impeded. The content, maintenance and use of an electronic mailbox are the responsibility of the person to whom the email account is assigned".

Example Two

There can be a temptation to use email informally, dispensing with the courtesies and attention to content required in conducting face-to-face or printed communications. However, it should be noted that once sent, email is irrevocable. Because of this, users should explicitly recognise their responsibility for the content, dissemination and

management of the messages they send. This responsibility means ensuring that messages:

1. Are courteous and polite.
2. Do not contain information that is harmful to the agency or employees (whether directly employed or contract staff).
3. Are consistent with other departmental policies, such as the Code of Conduct.
4. Protect other's rights to privacy and confidentiality.
5. Do not contain obscene, offensive or slanderous material.
6. Are not used for purposes that conflict with the agencies interests.
7. Contain an accurate signature.
8. Do not unnecessarily overload the email system.
9. Are not for commercial or personal purposes, unless authorised by the company.

Categories of behaviour and email deemed to be unacceptable are:

1. Networking of jokes with derogatory content and images of an offensive nature.
2. Posting sexual innuendos or personal information about others.
3. Sending messages that spread rumours about another employee.
4. Passing on material containing threats or violent fantasies."

Example Three[18]

"Computer work stations and the services accessible on them are provided to employees for business use to carry out tasks related to work. Services include email and the Internet. Reasonable private use of email and the Internet is permitted. However, it must be noted that this is a privilege and as 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. Every employee has a responsibility to be ethical and efficient in their official or private use of public property and services and to be productive in the use of their work time.

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:

1. Sex or age.
2. Pregnancy.
3. Race (including colour), nationality, descent or ethnic background.
4. Religious background.
5. Marital status.

[18] Also contains information on Internet use.

6. Disability.
7. 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 Australian or State regulations or laws. The Agency reserves the right to audit and remove any illegal material from its computer resources without notice.

Email is not to be intentionally used for chain letters. Employees are encouraged to report breaches of this policy to their supervisor or an appropriate senior officer or executive."

Accessing Personal Mail

The decision on whether or not to allow personal use of agency email is an individual decision for each agency. Whichever approach is adopted it should be both clearly stated and clearly understood. There are several *options* available:

1. Email may be used for incidental personal purposes[19]. It is permissible to use the email system for incidental personal purposes. This does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate agency policy with regard to employee time commitments or agency equipment.

2. Email may be used only for agency business. It is a violation of policy to use the agency's email system for any personal purposes.

3. It is unacceptable for a user to access personal email (such as Hotmail) using workplace computers.

Or maybe the agency will decide that:

4. It is acceptable for a user to access personal email (such as Hotmail) using workplace computers so long as the material being accessed is not prohibited by the agency's policy.

To ensure employees are aware that anything they access or open in web based email platforms can be scrutinised by the department, it should also be clearly stated that any webpage or email, including online emails such as "hotmail" are also subject to the department's acceptable use policy and guidelines.

[19] sometimes referred to as ephemeral email.

Internet Acceptable and Prohibited Use

Examples of content and issues that can be included for Internet use are given under three headings:

1. General
2. Acceptable
3. Not acceptable

General – Examples of Content

1. "Users should remember that existing and evolving rules, regulations, and guidelines on ethical behaviour of government employees, and the appropriate use of government resources, apply to the use of electronic communications systems supplied by State Government."

2. "Internet services are provided by the *Name of Agency* to support open communications and exchange of information, and the opportunity for collaborative government-related work. The *Name of Agency* encourages the use of electronic communications by its employees. Although access to information and information technology is essential to the missions of government agencies and their users, use of Internet services is a revocable privilege. Conformance with acceptable use, as expressed in this policy statement, is required."

3. "While the Internet contains much information that is useful for work purposes, it also contains significant volumes of information that may be interesting, but which is of limited direct use to the activities of *Name of Agency*. All officers should endeavour to maximise the value of their time on the Internet and avoid the unnecessary time and cost of 'surfing the net' when such activities add little value to work."

Acceptable

The issue of acceptable or appropriate use may be difficult to define in relation to Internet browsing. It may not be possible to tell if a web page is relevant until it has been read. Similarly, the operation of search engines can result in surprising and irrelevant search results, for example innocent words like chocolate can return sexually explicit sites. Links on web sites may also be misleading or irrelevant. Discussion with staff on the issue of work related web use might help to clarify the issue and identify what types of sites are in fact acceptable or relevant.

1. Personal Use

If an organisation determines that usage is to be work related only, it should clearly spell out what this actually means, and include examples or details of what is considered to be non-work related. For example:

a) The Internet may be used only for Agency Business. It is a violation of policy to use the Internet system for any personal purposes.

b) It is permissible to use the Internet for incidental personal purposes. This does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate agency policy with regard to

employee time commitments or agency equipment. Limited personal use 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 emailed to others.

The decision on whether employees may use Internet resources out of work hours for non-business related activities is a matter for individual agencies to decide. It is important to remember, even out-of-hours, the use of the agency's network reflects the agency's image. Potential liabilities will remain the same in case of serious infringement. If the restrictions placed on the types of content are different during work hours than during off hours, this should be clearly defined.

2. Other Acceptable Uses

Clearly determine what is regarded as acceptable use of the Internet, for example:

a) Communication and information exchange directly related to the mission, charter, or work tasks of the *Name of Agency*.

b) Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the user's government activities.

c) Use in applying for or administering grants or contracts for State Government research or programs.

d) Use for advisory, standards, research, analysis, and professional society activities related to the user's government work tasks and duties.

e) Announcement of new State laws, procedures, policies, rules, services, programs, information, or activities.

f) Any other governmental administrative communications not requiring a high level of security.

g) Communications incidental to otherwise acceptable use, except for illegal or specifically unacceptable uses.

h) Where a genuine business reason exists that requires access to sites that would be normally regarded as inappropriate, the authorisation of the Agency's Director General is required.

Unacceptable Use

Individual agencies will need to define what is unacceptable use for that particular agency. However, some general areas should be addressed, as they will generally be unacceptable, and include:

1. Use of the Internet for any purpose that violates Australian law or any Code or Policies, Standards and Procedures.

2. Use for any for-profit activities unless specific to the charter, mission, or duties of the State agency.

3. Use for purposes not directly related to the mission, charter, or work tasks of the State agency during normal business hours.

4. Use for private business, including commercial advertising.

5. Use for access to and distribution of:

    a) Indecent or obscene material.
    b) Pornography.

6. Use for access to, and distribution of, computer games that have no bearing on the agency's mission. Some games that help teach, illustrate, train in, or simulate agency-related issues may be acceptable. In this case, approval from agency management is required.

7. Use that interferes with, or disrupts, network users, services, or equipment.

8. Use of Internet services to seek out information, distribute information, obtain copies of, or modify files and other data, which is private, confidential, or not open to public inspection, or release such information unless specifically authorised to do so once the legal conditions for release are satisfied.

9. No intentional copy is to be made of any software, electronic file, program, or data without a prior, good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented.

10. Users shall not misrepresent themselves as other persons on the Internet, without the expressed consent of those other persons. Users shall not circumvent established policies defining eligibility for access to information or systems.

11. Use of Internet Services to develop programs designed to harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components of systems. Examples are viruses and Trojan horse programs.

12. Use for fundraising or public relations activities not specifically related to State Government activities.

13. It is not acceptable to take pornographic images from the Internet or from software and use as screensavers.

Other Issues

1. The Internet contains some information that is offensive. This includes hate mail, racist and pornographic material. While some agencies may have a legitimate reason for accessing some such material, most have no reason to access offensive material and all intentional access to such material should be prohibited.

2. Gambling via the Internet may also be a concern, and the policy should contain a prohibition against such activity not only because of its potentially adverse affect on productivity but also because the activity may be illegal.

3. Finally if there are particular applications of the Internet that your agency cannot provide for employees' personal use due to bandwidth restrictions, such as mailing lists or streaming media, these should be added to the paragraph about "What is not acceptable use".

Example One

1. Material of an offensive or obscene nature must not be posted or transmitted.
2. Impersonation of other users of the system is forbidden.
3. Forging of electronic signatures is forbidden.
4. Use of the Internet for commercial activities not directly pertaining to *Name of Agency* is forbidden.
5. The IT Team will monitor performance and impact and advise where services may need to be restricted. The Internet Administrator will keep the users informed.
6. Material which is libellous, defamatory or which discloses private or personal matters concerning any person must not be posted or transmitted.
7. Material that may violate the property rights of others, including unauthorised copyrighted text, images or programs, trade secrets or other confidential proprietary information, and trademarks or service marks used in an infringing fashion, must not be posted or transmitted.
8. Material, which contains viruses, worms, “Trojan horses”, or any other contaminating or destructive features, must not be posted or transmitted.
9. Material such as charity requests, petitions for signatures, chain letters or letters relating to pyramid schemes and broadcasting messages must not be posted or transmitted.
10. Users must not use the facilities and capabilities of the *Name of Agency* Internet services to conduct any activity or solicit the performance of any activity which is illegal or which infringes on the rights of others.

Example Two

1. All use of the *Name of Agency* computing and communication facilities, including the Internet, must be consistent with the purposes of the *Name of Agency*.

2. Access to, or use of, *Name of Agency* computing and communication facilities, including the Internet, for illegal or inappropriate purposes, or in support of such activities, is expressly forbidden.

    - Illegal activities are defined as any act which constitutes a violation of State or Commonwealth laws.
    - Inappropriate use is defined as any violation, of the conditions contained in the application forms or the terms and/or provisions contained in this standard.

3. Users must not knowingly violate copyright, licences agreements, or other contracts.

4. Users must not interfere with the intended use of information resources.

5. Users must not seek to gain or gain unauthorised access to information resources. Where access is gained accidentally, users must report to the information custodian, indicating the security breach.

6. Users must not use or knowingly allow another to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises, or representations.

7. Users must not without authorisation destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer-based information and/or information resources.

Acknowledgement of Obligations

A requirement for staff to sign a conditions of use statement, acknowledgement of obligations or similar, helps promote a common corporate understanding of acceptable use policies. For those agencies that wish to include this requirement, suggested content is:

1. "Officers to be given access to the Internet and/or email will first have to sign the Internet & Email Access - Acknowledgement of Obligations form. In signing this form, officers will acknowledge that they have read the Department's Information Technology Policy and, in particular, the policy on the Internet."

2. "Employees provided with access to the technical communications network must confirm in writing that they have read and understand the Agency's policy and guidelines on Internet and Email use."

An acknowledgement of obligations does not necessarily need to be written. Several government agencies are currently using electronic means to gain employees acceptance of their obligations. For example, an electronic 'pop-up' window can be used, which details the Acceptable Use policy and does not allow employees to progress unless they press the 'accept' button. This method is most commonly used at the initial login and can thereafter be used on a pre-determined basis to reinforce the policy, or to notify users of changes.

Monitoring

Government agencies are responsible for monitoring compliance with *all* internal policies. Monitoring the communications network is the most widely used method to ensure that email and Internet use policies are not being breached. Emails that are stored on the agencies systems can be monitored to detect patterns of misuse. Internet sites can be blocked (through the use of filtering software) and/or logs used to detect sites visited that contravene agency policy.

The policy should clearly set out the procedures in place for monitoring the email and Internet systems. This will include the detail of **what** information is logged and ***who*** in the organisation has rights to access the logs and content of staff email and Internet browsing histories. The agency should make it clear that it has the right to monitor, copy, access or disclose any information or files that are stored, processed or transmitted using agency equipment and services. It is the responsibility of the agency to:

1. Clearly outline the procedures and processes for monitoring staff compliance with the email and Internet in the policy itself.

2. Include details of the authorised person/s to undertake this function.

3. Employ adequate security protection between internal systems and the Internet.

4. Notify employees of the method used to confirm that employees are aware of, and understand the agency's policy and guidelines on email use.

5. Notify employees of their role in helping to make the agency's systems as secure as possible.

6. Clearly establish the process in the event of a breach of the policy.

7. Take responsibility to minimise unsolicited exposure by employees to inappropriate material via email, i.e. SPAM filtering.

Monitoring – Why

The agency may want to inform staff of the reasons for monitoring email and Internet use. This will help to ensure everyone in the agency is clear about the issues.

Example

"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:

1. Prevent de-standardisation of the computer network because of the downloading of unauthorised software.
2. Ensure compliance with agency policies.

3. Investigate conduct that may be illegal or adversely affect the agency or its employees.
4. Prevent inappropriate or excessive personal use of agency property.
5. Be able to link Internet sites accessed with the user identification.
6. Generate reports that link Internet sites with the user identification.

Monitoring – What

The agency needs to capture information that will enable it to evaluate the success of the policy, to determine if the policy has being breached, to support investigation and if necessary prosecution. The information that is to be monitored should be clearly identified and communicated to staff.

Example One

"Employee email boxes will normally contain the emails they have sent and received. Network back-ups and archives may also contain copies of emails that have been deleted by the user. As well as the actual content of messages, the date and time the message was transmitted, received and opened, as well as the email address of the sender and recipients will normally be recorded. All email traffic on the *Name of Agency* system is automatically logged and is subject to scrutiny by system administrators and auditors."

Example Two

"Audit logs will be used to monitor performance. The IT division will, where possible and practical switch on and record in audit logs all login attempts; unauthorised user privileges; and the switching of user Login ID's. All audit logs will be retained in a secure environment for a period of three months. IT will formally monitor usage quarterly, or as appropriate, using such reports as the top:

1. 50 active remote access users and top 50 inactive remote access users.
2. 50 users receiving the most external e-mails.
3. 50 users sending the most external e-mails.
4. 10 locations (domain places) that e-mails were sent from.
5. 10 locations (domain places) that e-mails were sent to.
6. 50 active Internet users.
7. 50 visited Internet sites.

The *Name of Agency* authorises review of data when there is:

1. Reason to believe that a violation of the law has occurred.
2. Reason to believe that a violation of this policy has occurred.
3. Suspicion that inappropriate behaviour has occurred.
4. Suspicion that facilities are compromised.

Example Three

"Name of Agency keeps and monitors logs of Internet usage that reveals information such as Internet servers (including World Wide Web sites) that have been accessed by employees, and the email addresses of those with whom they have communicated. *Name of Agency* will not:

1. Engage in real-time surveillance of Internet usage.

2. Monitor the content of email messages sent or received by its employees (unless a copy of such message is sent or forwarded to the Name of Agency by its recipient or sender in the ordinary way).

3. Disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law."

Monitoring – Who

Access rights to staff mail boxes and logs are normally restricted to those with responsibility for administering the system. Such access should be as limited as possible, and details of who has these access rights clearly set out in the policy. The policy should clearly outline the circumstances under which authorised staff can legitimately access employee emails and log files. It should indicate, in general terms, the circumstances under which an organisation will disclose the contents of emails and logs (e.g. to report a criminal or civil offence to the appropriate authorities).

Examples

1. "The CEO or staff specifically authorised by the CEO, may review or copy any email messages and may disclose messages to others."

2. "The Director General and the Team Leader Information Technology will monitor email and Internet management practices and report as appropriate".

Breaches and Consequences

The responsibilities and procedures for incident investigation should be clearly specified in the policy, and the responsibilities of all parities (staff and management) explained. Where there is a breach of the policy, it is the responsibility of the agency to deal with it promptly, appropriately and fairly. Procedures should be developed to determine if any inappropriate use is in breach of the agency's normal disciplinary guidelines and investigate whether formal disciplinary action should be taken.

Breaches

Examples of content that can be included in the policy to ensure all parties are clear on what constitutes a breach and what the associated procedures include:

Example One

"Every employee has a responsibility to be ethical and efficient in their official or private use of public property and services and to be productive in the use of their work time. Any identified use of equipment or services thought to be inconsistent with *Name of 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".

Example Two

"Staff shall report suspected breaches of the policy. In the case of a suspected breach, the Security Officer will:

- Obtain a detailed description of the event and its cause.
- Measure the impact and implications for the *Name of Agency* and authorised users.
- Review current policy and procedure to ensure that they are adequate.

For first breaches that are not serious:

- Staff will be formally notified and a record retained.

For repeat breaches and serious breaches, the Security Officer will:

- Advise the Director, Information Services
- Collect and retain system logs, audit trails and relevant file information
- Store offline all relevant information

The Director, Information Services will advise relevant business heads."

Consequences of Breach

Where inappropriate uses are identified, the agency has a responsibility to investigate these and where appropriate report them to the relevant authorities, for example notify the Police if it is reasonably believed that a criminal offence has been committed. Employees are responsible for reporting breaches and potential breaches of security as well as activities that are unethical or contravene the agency's guidelines or code of practice. The consequences of, and process associated with, a breach of the policy must be clearly stated, some examples include:

Examples

1. "If any use of the Internet services is found to be contradictory to *Name of Agency* policies the user may lose access privileges and disciplinary action may be taken."

2. "Violation of the Internet and email policy may result in a recommendation to revoke access to computing and communication facilities, result in disciplinary action, and where appropriate, referral to the WA Police Service".

3. "Suspension of service to users may occur when deemed necessary to maintain the operation and integrity of the *Name of Agency* network. User accounts and password access may be withdrawn without notice if a user knowingly violates the policy. Discipline may be appropriate in some cases of non-compliance with this policy. Criminal or civil action against users may be appropriate where laws are violated."

4. "The *Name of Agency* will review any alleged breach of this policy on an individual basis. If the alleged breach is of a very serious nature, e.g. breaching the employee's duty of fidelity to the agency, the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of the agency, the breach may be treated as grounds for dismissal. Otherwise, an alleged breach shall be dealt with as follows:

    a) Initially, the employee shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, be asked to desist from or where applicable to remedy the breach.

    b) If the breach is not desisted from or remedied, *Name of Agency* may either withdraw the employee's access to the Internet or provide a first warning to the employee, to which the employee shall have an opportunity to respond.

    c) If the infringing conduct continues the employee may be given a second and a third warning, to each of which he or she shall have an opportunity to respond.

    d) If a breach is committed after the third warning the employee may be dismissed."

5. "Suspected breaches of the policy will be investigated and resolved. A 'breach of discipline' is defined in Part X of the Prisons Act 1981 and in Section 80 of The *Public Sector Management Act 1994; and for other employees the discipline provisions applicable to their employment.* The relevant business head will conduct the discipline process in accordance with the existing disciplinary process."

Summary

The codes of conduct in use across the public sector make it clear that all employees have a responsibility to be ethical and efficient in their use of public property and services. This responsibility extends to the use of the Internet and email.

The Government is committed to ensuring email and Internet systems are used in an appropriate manner, and that both employers and employees are aware of the issues.

There are many issues that need to be taken into consideration when *developing, disseminating and enforcing* email and Internet use policies:

1. The policy development process needs to be inclusive and consultative.
2. The policy document needs to be clear and concise. It should be explicit and unambiguous. It should use plain language that can be readily understood by the intended audience. It should outline the scope, the objectives, and any procedural issues that need to be known by staff. The importance of specific issues such as acceptable and unacceptable uses, the monitoring and enforcement procedures, etc. will need to be covered.
3. There may be a requirement to supplement the policy document with guidelines to ensure that staff are fully aware of the rationale behind the policy decisions and the areas of concern, e.g. security, privacy, etc.
4. The policy needs to be consistent with other internal policies.
5. How the policy is to be communicated to staff should be considered. This will need to include dissemination for new staff and for existing staff when amendments are made.
6. There will be a need to ensure processes and procedures that underpin the policy are developed. For example, there may be a need to install appropriate technology.
7. The policy will need to be monitored, reviewed and updated.

Although many of the issues that surround Internet and email use policies will be the same in all agencies, such as security, records keeping requirements, etc., there may be procedural and process issues that will be specific to individual agencies. Individual agencies will need to make strategic decisions based on their specific needs and requirements. These Guidelines will assist in the development of policies, but are not a replacement for strategic decision-making. Once decisions have been made, agencies will find that the policy development process will be more effective and less arduous.