DISCLOSED UNDER FOI

Guidelines on the use of Information Technology and Internet Services (May 2001)

1. Authorised use of information technology

Information technology (IT) facilities are provided by the Ombudsman's office ("the office") only for the purpose of enabling authorised users to conduct government business, or performing the functions of the Ombudsman's office. These facilities include all computer and computer-related facilities, Internet connections, internal and external electronic mail, telephones and facsimiles. Authorised users include officers and contract staff specifically authorised to make use of the office's IT facilities.

When using IT facilities to conduct government business, or functions of the Ombudsman's office, users should be sensitive to the nature of information being accessed or created and ensure that appropriate security is involved in saving, copying or transmitting data.

Authorised users are not permitted to make use of the office's IT facilities for unacceptable uses. Unacceptable uses are described below. The office will accept incidental personal use of IT facilities provided that its impact on the office is negligible. Guidance on incidental personal use is provided below.

top

2. Unacceptable uses

Unacceptable uses of the office's IT facilities include:

- any use in breach of a Commonwealth law or the Australian Public Service (APS) Code of Conduct
- distributing material that is harmful to, or that conflicts with, the interests of the Commonwealth or the office
- breaching intellectual property rights, including copyright on software
- interfering with the authorised use of the IT facilities by others

DISCLOSED UNDER FOI

- intentionally disrupting the operation of the IT facilities, spreading viruses with intent to cause harm or gaining unauthorised access to a computer system
- gaining unauthorised access to information and/or altering, deleting, inserting, or damaging that information
- using the IT facilities for private commercial activities, or private activities such as 'on-line' gambling, or advertising such as in relation to political activity[1]
- intercepting another person's communications or e-mail without permission from the individual, or without the direction from the individual's manager
- importing, creating, intentionally accessing, possessing or distributing any offensive, obscene or indecent images, data or other material including material which has as its main focus pornography, nudity or sexual acts
- distributing defamatory, abusive, sexist or racist material or material likely to promote conflict or to incite violence against identifiable groups
- distributing chain letters
- distributing e-mail anonymously, using a false identity or using another person's user identification
- using internal contact lists, addresses or e-mail contacts for personal circulation (i.e. for non-official purposes) to external organisations or individuals
- distributing communications or e-mail that disclose personal information (including telephone numbers or e-mail addresses) without appropriate authorisation
- intentionally using the IT facilities to harass, intimidate, threaten or offend another person.

top

3. Advice

Further information and advice on the interpretation of these guidelines should be sought in the first instance from your regional manager. Advice should always be sought in cases where there is doubt as to whether a particular use is unacceptable or not.

While e-mail should not be used to disseminate union material, office management may sanction its use for specific activities such as negotiation of the office's certified agreement.

The use of IT facilities for personal financial transactions, such as internet banking for convenience, is permitted on the understanding that the responsibility for the transaction is solely your responsibility and is undertaken in your own time. This includes responsibility for transaction content and technical support. The Ombudsman's office will not be held liable for any financial loss incurred though using the office facilities for personal financial transactions, whether the loss is due to systems failure or any other reason. Staff need to ensure that this type of transaction does not disrupt the operation of the IT facilities or interrupt on-going office work.

4. Responsibility

All members of staff in the office who use the IT services such as e-mail and the internet are responsible for:

DISCLOSED UNDER FOI

- contents being generated by your e-mail account
- managing your e-mail environment by deleting all unnecessary or unsolicited material from your account at the earliest possibility
- actively discouraging the use and circulation of 'junk' mail
- not altering or dismantling equipment without proper authority
- not attempting to remove or avoid security processes within the IT services and equipment
- notifying supervisors or appropriate managers of any perceived misuse of IT services
- securing your workstation from improper use, by regularly changing your password, not passing your password to other people, activating secure screen-saver and shutting your workstation down at the end of the working day.

top

5. Complaints and investigation

Instances of unacceptable use of the office's IT facilities should be reported in the first instance to your manager. Where the unacceptable use involves issues you believe fall within the office harassment guidelines you should bring the matter to the attention of your local harassment contact officer. Complaints will be investigated by the Director of SSIMU or management in the first instance or, where necessary, referred to the Australian Federal Police. Where it involves harassment it will be handled in accordance with the harassment guidelines.
6. Sanctions for non-compliance A breach of these guidelines may result in disciplinary action (including dismissal) under the Public Service Act or criminal prosecution or both.

top

7. Monitoring of electronic networks

Authorised users should be aware that their use of IT facilities may be monitored for operational reasons to determine whether the network is operating efficiently and there are no security breaches. To protect the security of the system and to isolate and resolve problems, this activity can involve the removal of material from the network and/or the removal of user access.

E-mail and internet usage is routinely monitored. Records of transactions can be obtained in cases of concern or complaint. These records include the e-mail sender and recipient addresses, and time of transmission. The content of the email would not normally be recorded but may be stored on mail servers, backups or archives. With web browsing, the addresses of sites visited, the date and time they were visited and the duration of site visits may be logged. Users should be aware that session content from browsing may be stored in the memory of network servers and desktop equipment.

A limited number of IT support staff (Director of IT, and the Network System Administrator) have access to these records as part of their operational duties and the extent of this access will not exceed the minimum essential for performance of these duties. Normal routine

DISCLOSED UNDER FOI

analysis will not involve reading the content of electronic messages or files. However, if due to routine analysis or a complaint the Director of IT or Network Systems Administrator reasonably suspects that an authorised individual is misusing the facilities, further investigation and action may involve special monitoring and/or reading the contents of individual electronic messages and files. Any such investigation will be conducted in accordance with the Privacy Act 1988 and other relevant legislation.

The office has the capability to investigate the origin and destination of telephone and facsimile calls made from the office PABXs. Information recorded includes the origin of the call, called number, duration, and time of day. Telephone and mobile phone accounts are routinely monitored to identify billing errors and patterns of excessive use, and to certify expenditure.

Staff should also be aware that all e-mail, files and telephone records may be inspected by authorised IT support staff for the purpose of responding to external persons (for example, FOI requests) or to bodies such as the Australian Federal Police or the courts. The content of e-mail and files may also be inspected for the purpose of advising the office management or in response to internal investigations.

top

8. Incidental personal use

The office recognises that staff may occasionally wish to take advantage of the convenience of e-mail, the internet and IT facilities generally for personal purposes. In seeking to maintain a balance between the needs of the office and the needs of staff, and with regard to the proper use of public funds, the Ombudsman will accept incidental personal use of IT facilities provided that: (i) it does not constitute an unacceptable use as detailed above; and (ii) its impact on the operations of the office is negligible.

Staff should bear in mind the following aspects, which may represent costs to the office of such personal use:

- the time spent in composing, reading, reviewing
- time spent in surfing the internet, especially when following up false leads or distracting internet sites
- the use of facsimile and printer resources: paper, toner and maintenance
- the use of other resources (server storage space, network traffic, equipment memory with attachments or downloads of high volume objects such as pictures/video etc)
- the interruption to the flow and pattern of work
- occupational health issues related to excessive time spent at a computer screen and keyboard
- impact on the work of colleagues, particularly how colleagues may feel about receiving unsolicited e-mails
- the risks of viruses, worms, etc: being transferred to computers in the office
- the risks of leakage of official information by staff visiting unscrupulous Internet sites, which may interrogate the browsing workstation.

DISCLOSED UNDER FOI

Whilst it is difficult to establish what is a reasonable level of incidental personal use, staff should take note of these indicators:

- intrusion into one's ability to fulfil required duties is unacceptable
- personal use of IT facilities should preferably be confined to times which are outside of normal working hours
- use outside of normal working hours for the pursuit of study or research etc from which the office or Commonwealth will benefit, is viewed with greater acceptance.

There can be situations where the mere association of a statement or opinion with the name of the office may appear to give an endorsement or authority that is not intended or is inappropriate. Staff must take care not to create such a situation. Staff should bear in mind that the mere inclusion of their e-mail address on distribution lists of some organisations (e.g. clubs, political groups) may create an impression that is not consistent with the image of the office or Commonwealth. Staff should use home e-mail addresses for such purposes.

Staff should note that, whilst the sharing of jokes, etc can contribute to the maintenance of morale, some staff find these intrusive, and their distribution should be kept to a minimum. Jokes that may be offensive, obscene or otherwise indecent should never be distributed using facilities provided by the office.

Staff should also note (as discussed earlier) that most e-mail is not secure. It should be regarded as accessible unless it has been encoded or encrypted. E-mail is often compared to a postcard in that anyone who receives it can read it. E-mail may also be read if it is stored on servers during transmission. E-mails are hard to destroy. Many people think that if they delete their e-mail it is gone forever. This is not so as most electronic documents are backed up and recoverable. Also most networks have transaction logs, and these logs will normally include the e-mail addresses of senders and recipients of e-mail and the time of transmission. The content of e-mails themselves would not normally be logged but may be stored on mail servers. Similarly, web server logs record information on the sites that people visit.

The keeping of these logs is usually necessary for the routine maintenance and management of networks and systems.

top

9. Review

These guidelines will be reviewed after any major changes, such as in government policy, business requirements or the information technology environment, to ensure that they remain relevant. Requirements, suggestions and comments in regard to these guidelines should be forwarded to the Director of IT.

All staff are required to acknowledge that these guidelines have been read. This can be done by printing the acknowledgment page linked below, or by signing an acknowledgment page supplied by the Help Desk. The acknowledgement needs to be forwarded to the Help Desk upon completion (internal mail). Please contact the Help Desk if you have any questions.

DISCLOSED UNDER FOI

[1]Commercial activities' in this context are defined as activities aimed at providing a profit. It includes activities such as share-trading. 'Political activity' is defined as 'exercising or seeking power in the governmental or public affairs of a state, municipality, or the like' (Macquarie dictionary)