Department of
Education

TELECOMMUNICATIONS USE

EFFECTIVE: 1 AUGUST 2003

CONTENTS

1 POLICY 3
2 BACKGROUND 3
3 PROCEDURES 4
3.1 ONLINE SERVICES 4
3.2 TELECOMMUNICATIONS SECURITY 4
3.3 COMPUTER VIRUSES 5
3.4 TELEPHONES 5
4 RELEVANT LEGISLATION AND AUTHORITY 5
4.1 RELATED DEPARTMENT POLICIES 5
APPENDIX A GUIDELINES 6
A.1 SECURITY AND PRIVACY 6
A.1.1 PASSWORD PROTECTION 6
A.1.2 SECURITY LABELS 6
APPENDIX B COPYRIGHT NOTICE 8

1 POLICY

Staff and contractors of the Department of Education must only use telecommunication resources, including computer hardware, Internet, intranet, electronic mail, faxes, telephones (fixed and mobile), for purposes that are legal, ethical and consistent with the aims, values and ethos of the Department. Staff must not deliberately access, download, store or send materials of a pornographic, racist, sexist, inflammatory, hateful, obscene or abusive nature.

Personal use of telecommunication resources is permitted provided it is not for commercial gain or in any way counter productive to the business of the Department.

Staff and contractors of the Department of Education must treat electronic messages sent or received in the course of business transactions as public records. These messages are subject to the Department's Records Management Policy in the same way as any other Departmental records.

Principals must ensure that procedures are developed to manage student use of on-line services such as email, the Internet and other web-based services at their school.

Line managers are responsible for the management of telecommunications resources.

2 BACKGROUND

This policy applies to all Departmental work places including schools and to all employees, whether permanent, temporary or on contract. It also applies to commercial contractors undertaking work on behalf of the Department.

The Department will exercise its right to review, audit, intercept, access and disclose messages created, received or sent over Departmental 'on-line services', defined here as: any services, such as, but not limited to, email, discussion groups, Internet access and Web browsing, that may be accessed using the computer networks and services of the Department of Education. Logs of email transactions and Internet access data are kept for administrative, legal and security purposes and may be monitored.

Like any other corporate records, emails and Internet access records are 'discoverable' in the event of legal action and are subject to provisions of the Freedom of Information Act. Discovery is the process by which parties to a civil case or matter are entitled to obtain, within certain defined limits, full information of the existence and the contents of all relevant documents relating to the matters in question between them.

Records Management: Policy and Guidelines (1997) should be consulted in relation to the destruction or archiving of electronic messages classified as significant records.

3 PROCEDURES

3.1 ONLINE SERVICES

a) Staff and contractors must restrict their usage of Departmental online services for personal reasons, and use discretion in the content involved. Such usage must not:

- interfere with the employee's job functions;
- place undue demands on the network;
- involve deliberately accessing, sending or downloading of materials that are unacceptable in terms of legislation, Public Sector and Department policy. This includes material that carries content that may be considered to be of a pornographic, racist, sexist, inflammatory, hateful, obscene or abusive nature;
- involve transmission of:
  - messages of a party political nature;
  - unsolicited advertising material;
  - messages of personal commercial benefit;
  - chain letters;
  - personal broadcast messages;
  - intentional harassment; or
  - materials intended to harm or discredit any individual or group.
- involve bulk electronic mailing of non work-related messages to groups of users without the approval of a manager or principal;
- involve wilfully or repeatedly opening email or email attachments from suspicious or untrustworthy sources, or, bypassing the Department's anti-virus defences.

b) Staff and contractors must ensure confidentiality, integrity and security of electronic messages.

c) Staff and contractors must ensure that their Departmental Internet access or email accounts are not shared or used by other officers.

d) Approval to send bulk electronic mailing of messages to groups of users must be obtained from principals if at schools, the director if at a district office or the Executive Director if at central office.

e) All global email to schools must have the approval of the Office of the Director General.

f) The context or content of electronic records must not be altered or manipulated once created or received.

Copyrighted materials being transmitted by email must be in accordance with the *Copyright Amendment (Digital Agenda) Act 2000* and must be accompanied by an electronic copy of the Form of Notice per paragraph 135ZXA(a) of the *Copyright Act 1968*. A copy of this attachment is shown at Appendix B.

Guidelines
Detailed guideline information is available in Appendix A.

3.2 TELECOMMUNICATIONS SECURITY

a) Staff and contractors must not gain unauthorised access, or attempt to access, other computers or networks.

b) Staff and contractors must not allow or facilitate unauthorised access to the Department's network through the disclosure or sharing of passwords, personal logon information, user accounts or other information designed for security purposes (see ICT Security Standard 1.2 User ID and Password).

3.3 COMPUTER VIRUSES

a) Staff and contractors must not initiate the propagation of computer viruses or other malicious software or attempt to bypass the mandated virus protection software in use by the Department.

b) Staff and Contractors must comply promptly with instructions from the Customer Service Centre regarding treatment of viruses.

3.4 TELEPHONES

a) Employees must ensure the most economical use possible of telephones.

b) Managers must ensure that cancellation of service is notified to the service provider.

c) Employees must have the written permission of their line manager before obtaining a Departmental mobile telephone.

d) Line managers must satisfy themselves that mobile phones are allocated to staff on the basis of need or benefit.

e) Line managers must ensure that the selected usage plan is the most economical for their pattern of use.

f) Employees must pay for calls not related to their work requirements made on departmental mobile telephones.

g) Loss of a mobile phone must be immediately reported to the employee's line manager.

4 RELEVANT LEGISLATION AND AUTHORITY

Public Sector Code of Ethics

The Public Sector Management Act 1994

The Copyright Amendment (Digital Agenda) Act 2000

4.1 RELATED DEPARTMENT POLICIES

Code of Conduct

Information Privacy and Security

Copyright for Schools

APPENDIX A GUIDELINES

Those creating or receiving email messages need to decide whether a message is a record and therefore to be preserved. This requires the same judgement as that applied in determining whether to retain and file paper records.

Table 1 will assist users to determine the value of and retention requirements for email messages.

Type of message	Value	Retention
Transactions that provide evidence of business activities, e.g. directives, development of policy issues	Significant records required for ongoing business	To be retained in accordance with the approved retention and disposal schedules. These records must be included in a records keeping system.
Information messages with a business context but not part of a business transaction, e.g. notification of a meeting, a message containing an attached document or personal or social messages.	Records of ephemeral value	Destroyed when not required. While retained on the Department's electronic mail system, they are subject to legislation such as the Freedom of Information Act and legal processes.

Table 1: email retention guidelines

Based on Email is a record! Archives advice 20. Australian Archives. Reproduced by permission of the Australian Archives.

A.1 SECURITY AND PRIVACY

Although it gives the *illusion* of being private, caution is needed when dealing with email. Even after a user deletes an email from the system it may still exist on disk or back-up facilities. Email messages can be saved indefinitely on the receiving computer and copies can easily be made and forwarded to others, either electronically or in paper form.

The security and authenticity of records communicated through email systems may be maximised by using:

A.1.1 PASSWORD PROTECTION

- Restrict access to a system or application to authorised users, and choose passwords that are difficult for people or computer programs to guess (see Annex B to ICT Security Standard 1.2 User ID and Password); and

A.1.2 SECURITY LABELS

- Attach labels such as 'urgent', 'confidential' or 'acknowledgment requested' to alert recipients to the need for special privacy and handling requirements.

For more information in relation to security, password protection and the classification of information, staff are advised to refer to the *Information Privacy and Security* (2000) policy and ICT Security Standards.

APPENDIX B COPYRIGHT NOTICE

ATTACHMENT 'E'

(TO BE ATTACHED TO ALL ELECTRONIC AND COMMUNICATED COPIES OF COPYRIGHT MATERIAL)

FORM OF NOTICE FOR PARAGRAPH 135ZXA (a) OF THE COPYRIGHT ACT 1968

COMMONWEALTH OF AUSTRALIA

Copyright Regulations 1969

WARNING

This material has been reproduced and communicated to you by or on behalf of [*insert name of school, district office, Central Office*] pursuant to Part VB of the *Copyright Act 1968* (*the Act*).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.

THE ABOVE NOTICE FORMAT SHOULD BE COPIED AND PASTED INTO THE DOCUMENT