
ACCEPTABLE USE POLICY

FOR

INTERNET, EMAIL AND OTHER ELECTRONIC COMMUNICATIONS

1. Scope

- 1.1 This policy applies to the users of the DE&T network or DE&T equipment, which includes but is not limited to all staff, contractors, casuals, temporaries and volunteers of DE&T, all schools, regions and school councils.
- 1.2 Use of the DE&T network includes transmissions to or through the DE&T network by a party described in paragraph 1.1.
- 1.3 This policy governs the use of all electronic communications (excluding telephones), and includes but is not limited to:

Publishing and browsing on the Internet (including Intranet and Extranet) and Electronic mail ('Email'),
Electronic bulletin/notice boards,
Electronic discussion/news groups,
File transfer,
Video conferencing,
Streaming media,
Instant messaging, and
'Chat' facilities.

all of which are referred to in this document as "Electronic Communications".

- 1.4 Any reference in this policy to an Act, law, Code of Conduct or other document includes a reference to the Act, law or document as amended from time to time.
- 1.5 In this policy, -
- (i) an "Authorised Person" means a person authorised by the Secretary to the Department of Education & Training,
 - (ii) "copyright" does not include moral rights under the Copyright Amendments (Moral Rights) Act 2000.
 - (iii) "Guidelines for the Classification of Films and Videotapes (Amendment No 3)" mean the Guidelines approved by the Commonwealth, State and Territory Ministers in accordance with section 12(3) of the Commonwealth (Classifications Films and Computer Games) Act 1995 on 18 September 2000.
 - (iv) "Personal use" means all non work related use, and includes usage for entertainment, games, general news, gambling, communicating or involvement with unions, professional bodies or other employee representatives, hobbies, glamour, investments, Job search, motor vehicles, personal/dating, real estate, shopping, sports, travel, UseNet/News, and private emails

2. Purpose

- 2.1 The purpose of Electronic Communications within DE&T is to conduct the business and functions of DE&T.
- 2.2 The purpose of this Policy is to ensure that Electronic Communications are properly and efficiently used, and that the Department is protected from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

3. Rationale

- 3.1 The use of Electronic Communications at DE&T carries with it responsibilities.
- 3.2 Publishing, accessing information and communicating electronically can be cost-effective, timely and efficient. It is essential that use of this valuable resource be managed to ensure that it is used in an appropriate manner.
- 3.3 The process by which DE&T seeks to manage staff use of Electronic Communications is through the development and implementation of this Policy. The Policy provides specific instructions, which must be followed whenever using Electronic Communications.

4. Responsibility

- 4.1 It is the responsibility of General Managers, Managers, and Principals to ensure that the persons to whom this Policy applies are aware of this Policy. This should include, but is not limited to -

- (a) providing a copy of the Policy,
- (b) regular and timely reminders of the need for compliance with the Policy,
- (c) providing updates or developments of the Policy,

to those affected by the Policy.

- 4.2 It is the responsibility of individuals to abide by the Policy.

5. Non-Compliance

- 5.1 Non-compliance with this Policy -

- (i) may constitute a criminal offence, inappropriate behaviour, pose a threat to the security of the DE&T network, the privacy of staff and other persons and may expose the users of the system or other persons to legal liability, and
- (ii) will be regarded as a serious matter and appropriate action will be taken when a breach of the policy is identified,

- 5.2 Breaches of this policy -

- (i) will generally be categorised using the categories and guidelines in paragraph 20, and

- (ii) may result in disciplinary action including revoking or restricting any right to use Electronic Communications, cautioning, or, in appropriate circumstances, may lead to more serious disciplinary action including termination of employment and possible reporting to the police.

6. Business Purposes

- 6.1 DE&T's Electronic Communications network is a tool to be used for DE&T purposes.
- 6.2 Electronic Communications must –
 - (a) only be used for DE&T purposes, or where authorised or required by law, or with the express permission of an Authorised Person, and
 - (b) be used like other business communications and comply with any codes of conduct which apply to the user, such as the Code of Conduct for the Victorian Public Sector, and Teaching Service Orders.
- 6.3 Users of the DE&T network may use Electronic Communications for personal use, provided the use is not excessive. Users must not engage in excessive personal use during working hours, or excessive personal use outside working hours. A breach of either of these constitutes a failure to abide by this policy. Personal use is defined in clause 1.5, and categories 4 and 5 in clause 20 provide further details of what will generally be considered to be "excessive".
- 6.4 Subject to limited personal use in accordance with clauses 6.3 and 20 -
 - (i) subscribing to list servers (LISTSERVS), mailing lists and other like services must be for DE&T purposes or professional development reasons only, and
 - (ii) on-line conferences, discussion groups or other like services must be relevant and used for DE&T purposes or professional development activities. Such interaction requires that Internet etiquette should be observed along with current societal standards for respect and fairness.
- 6.5 Obtaining unauthorised access to electronic files of others, or to Email or other Electronic Communications of others, is not permitted.
- 6.6 Large downloads or transmissions should be minimised to ensure the performance of Electronic Communications of other users are not adversely affected.

7. Department Property

- 7.1 DE&T is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through DE&T's network.
- 7.2 Electronic Communications created, sent or received by the users referred to in paragraph 1.1 are the property of DE&T, and may be accessed as records of evidence in the case of an investigation. Electronic Communications may also be subject to discovery in litigation and criminal investigations. For example, all information

produced on computer, including Emails, may be accessible under the *Freedom of Information Act*. Email messages can, and have been, retrieved from back up systems and organisations, their employees and the authors of Email have been held liable for Email messages that have been sent.

8. Monitoring

8.1 Electronic Communications will be treated as DE&T related and may be monitored by Authorised Persons.

8.2 From time to time Authorised Persons may examine the records of Electronic Communications including for operational, maintenance, compliance, auditing, security or investigative purposes. For example, monitoring may occur of web sites visited, the contents of Email may be required by law to be disclosed or DE&T may investigate a complaint arising from the use of Email.

8.3 Electronic Communications are provided to you on condition that you agree to monitoring in accordance with this Policy. Your use of Electronic Communications constitutes your consent to monitoring in accordance with this Policy.

9. Defamation

9.1 Electronic Communications must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or DE&T liability. Electronic Communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and extremely widespread.

10. Copyright Infringement

10.1 The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, text and down loaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing copyright material by electronic means, may give rise to personal and/or DE&T liability, despite the belief that the use of such material was permitted.

10.2 DE&T supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.

10.3 All users of Electronic Communications must ensure they are familiar with the following publications issued by DE&T :

- (a) *Guidelines on Copyright and Trademark Management*; and
- (b) *Copyright for Schools*

11. Illegal/and offensive material

- 11.1 Electronic Communications must not be used in any manner contrary to law or likely to contravene the law. Any offender will be referred to the police or other relevant authority and their employment may be terminated.
- 11.2 Material must not be accessed or distributed in any manner contrary to law. This includes defamatory, racially vilifying, pornographic or unlawfully discriminatory material.
- 11.3 In particular, DE&T is an institution charged with the safety and education of children, and child pornography is both abhorrent and represents the antithesis of our responsibilities to children. Any offender will be referred to the police and their employment may be terminated.

12. Confidentiality

- 12.1 Electronic Communication is not a secure means of communication. While every attempt is made to ensure the security of DE&T's computer network, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

13. Viruses

- 13.1 Electronic Communications are potential delivery systems for computer viruses. All data, programs and files which are downloaded electronically or attached to messages should be run through a virus scan program before being launched, or opened or accessed.
- 13.2 Viruses have the potential to seriously damage DE&T's network. Do not open any downloaded files or Emails or attachments that you are not expecting or that look suspicious. In the event that you receive any files that you suspect contain a virus it should be reported immediately to your line manager.

14. Inappropriate content

- 14.1 The author and/or DE&T may be liable for what is conveyed in electronic communications. Electronic Communications, whether sent internally or externally, must only contain content that is appropriate to a work place environment.
- 14.2 Electronic Communications must not be used to publish, send or distribute material that is harassing, obscene or threatening, nor may it contain content that may be considered unlawfully discriminatory, offensive or disruptive. This includes sexually oriented messages or images and sexual harassment messages. All users of Electronic Communications should be familiar with '*Rights and Responsibilities under the Victorian Equal Opportunity Act 1995: training for principals, staff and school councils*'.

15. Attribution

- 15.1 There is always a risk of false attribution of Electronic Communications. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. At any stage if a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an Electronic Communication has been intercepted or modified, the line manager or principal should be informed.
- 15.2 Users are accountable for all use of DE&T systems performed with their user-ID. User-ID's and password must be kept secure and confidential. When students access a teacher's computer or use a generic user-ID as part of the school's learning program, teachers should maintain proper supervision and monitoring of the student's activities.
- 15.3 Active connections are to be terminated when access is no longer required and PCs secured by password when not in use.

16. Mass distribution

- 16.1 The use of Electronic Communications for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited.
- 16.2 Mass Electronic Communications should only be sent in accordance with normal DE&T procedures.

17. Records Management

- 17.1 Electronic Communications are public records and subject to the provisions of the *Public Records Act 1973*.
- 17.2 DE&T record management practices for management of Email messages must comply with the Interim Guidelines for the management of Electronic Mail messages of September 1999 ("The Guidelines"). All users of Email must be familiar with *DE&T's 'Recordkeeping Policy and Guidelines, June 1999'*.
- 17.3 Email messages that are routine or of a short term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records. For more information see The Guidelines and DE&T checklists for the retention or disposal of electronic messages for DE&T.
- 17.4 Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be maintained in a user's Email account.

18. Disclaimer

- 18.1 All Emails sent externally from DE&T's Edumail service will automatically have a disclaimer attached to them. The present disclaimer is worded as follows.

' IMPORTANT - This email and any attachments may be confidential. If received in error, please contact us and delete all copies. Before opening or using attachments, check them for viruses and defects. Regardless of any loss, damage or consequence, whether caused by the negligence of the sender or not, resulting directly or indirectly from the use of any attached files our liability is limited to resupplying any affected attachments. Any representations or opinions expressed in this email are those of the individual sender, and not necessarily those of the Department of Education & Training.'

- 18.2 This disclaimer must not be altered or interfered with in any way, except by Authorised Persons. The use of this disclaimer may not necessarily prevent DE&T or the sender of the Email from being held liable for its contents.

19. Complaints

- 19.1 If you receive an internal or external Electronic Communication which is offensive or inappropriate, raise it with your line manager, or the DE&T Complaints and Investigations Unit if your line manager is the cause of your complaint.

20 Breaches of this policy

Breaches of this policy will generally be categorised using the following categories and guidelines. The categories do not cover all breaches of this policy, for example the categories do not specifically refer to breaches of copyright under paragraph 10.2. Matters not covered by the following categories will be dealt with on an individual basis and on the relevant facts.

Category 1 : Illegal

This category covers the following.

- a. **Child pornography** - ie accessing, printing, transmitting, or possessing (including storing) child pornography. These offences are in section 70 of the Crimes Act 1958 and 57A of the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995.
- b. **Objectionable material** - ie transmitting or distributing "objectionable material" or any "objectionable publication" within the meaning of sections 32 and 57 of the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995. This covers material that has or would attract a classification of **X18** or **RC** under the Guidelines for the Classification of Films and Videotapes (Amendment No 3).
- c. Any other material or activity which involves or is in furtherance of a breach of the criminal law.

Category 2 : Extreme

This category involves accessing or storing material that has or would attract a classification of **RC** under the *Guidelines for the Classification of Films and Videotapes (Amendment No 3)*. This covers any material that:

- a. deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that reasonable adults would consider the material offends against standards of morality, decency or propriety generally accepted by adults to the extent that the material should not be classified,
- b. depicts a child under 16 years of age in a way that is likely to cause offence to a reasonable adult, or
- c. promotes, incites or instructs in matters of crime or violence.

Category 3 : Critical

This category involves accessing or storing offensive material. This covers any material that:

- a. Has or would attract a classification of **X18** under the Guidelines for the Classification of Films and videotapes (Amendment 3). The material covered by this classification is only available for hire or sale in the ACT and NT, and covers sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults.
- b. Involves racial or religious vilification
- c. Is unlawfully discriminatory
- d. Is defamatory
- e. Involves sexual harassment, or
- f. brings or has the potential to bring the employee or Department into disrepute.

Category 4 : Excessive personal use during working hours.

This category covers personal use which satisfies the following 3 criteria -

- a. it occurs during normal working hours (but excluding the employee's lunch or other official breaks), and
- b. it adversely affects, or could reasonably be expected to adversely affect the performance of the employees duties, and
- c. the use is more than insignificant.

Category 5 : Excessive personal use outside working hours.

This category covers personal use outside normal working hours (which covers the period before work, lunch and other official breaks, and after work).

Generally, personal use of 2 or more hours on a particular day will be considered excessive for category 5, except where the employee exceeds that time when acting within a learning or familiarisation program endorsed by the employee's manager or principal.

21. Replacing previous policies

21.1 This policy replaces the 2001 DE&T Acceptable use policy for internet, email and other electronic communications.

21.2 It does not replace the policy issued to schools titled "Safety Net, Internet Usage - Guidelines for Schools".

Effective: September 2002

Updated: September 2002