

# ACCEPTABLE USE POLICY

## FOR

### DEPARTMENT OF EDUCATION & TRAINING INFORMATION, COMMUNICATIONS AND TECHNOLOGY (ICT) SYSTEMS

#### 1. Purpose

---

- 1.1 The purpose of this Policy is to ensure that all use of the Department of Education & Training's Information, Communications and Technology (*ICT*) systems is legal, ethical and consistent with the aims, values and objectives of DE&T.
- 1.2 DE&T ICT systems must be properly and efficiently used. DE&T ICT systems are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, sexual harassment, stalking, illegal activity and privacy violations.

#### 2. Scope

---

- 2.1 In this Policy –
- (i) an “Authorised Person” means the Secretary or a person authorised by the Secretary of the Department of Education & Training;
  - (ii) “copyright” does not include moral rights under the *Copyright Amendment (Moral Rights) Act 2000* (Cth);
  - (iii) “DE&T” means the State of Victoria – Department of Education & Training;
  - (iv) “DE&T ICT systems” includes but is not limited to, DE&T Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, Internet, electronic mail (*Email*), computer systems, software, servers, desktop computers, notebook computers, leased notebook computers, mobile phones, digital cameras, hand held devices (for example, personal digital assistants or “PDAs”), USB Memory sticks and other ICT storage devices;
  - (v) “electronic communications” means Email, instant messaging and any other material sent electronically;

- (vi) “Guidelines for Classification of Films and Computer Games 2005” means the *Guidelines for Classification of Films and Computer Games 2005* made in accordance with sub-section 12(3) of the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) and effective from 26 May 2005.
- (vii) “personal use” means all non-work related use, and includes Internet usage and private Emails.
- (viii) “users” of DE&T ICT systems includes all employees (including ongoing, casual and temporary employees) and contractors engaged by DE&T, school councils, schools, regional offices and district offices. It also includes all volunteers of DE&T, school councils, schools, regional offices and district offices who use DE&T ICT systems.

2.2 This Policy applies to all users of DE&T ICT systems regardless of work location.

2.3 This Policy applies to the use of all aspects of DE&T ICT systems, networks, software and hardware collectively referred to as “**DE&T ICT systems**” (see definition of “DE&T ICT systems” in clause 2.1).

2.4 Use of DE&T ICT systems includes transmissions to or through DE&T ICT systems by a user.

2.5 This Policy governs the use of DE&T ICT systems and includes but is not limited to:

- Publishing and browsing on the Internet (including Intranet and Extranet);
- Downloading or accessing files from the Internet or other electronic sources;
- Email;
- Electronic bulletins/notice boards;
- Electronic discussion/news groups;
- Weblogs (‘blogs’);
- File transfer;
- File storage;
- File sharing;
- Video conferencing;
- Streaming media;
- Instant messaging;
- Online discussion groups and ‘chat’ facilities;
- Subscriptions to list servers, mailing lists or other like services;
- Copying, saving or distributing files;
- Viewing material electronically; and
- Printing material.

2.6 Any reference in this Policy to an Act, Regulation, Guidelines, Code of Conduct or other document includes a reference to the Act,

Regulation, Guidelines, Code of Conduct or other document as amended from time to time.

### **3. Rationale**

---

- 3.1 The use of DE&T ICT systems carries with it responsibilities.
- 3.2 The provision of DE&T ICT systems by DE&T is to improve and enhance learning and teaching, and conduct of the business and functions of DE&T. Using information technology, 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 DE&T ICT systems is through the development and implementation of this Policy. The Policy must be followed whenever using DE&T ICT systems.

### **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 may include, but is not limited to -
  - (a) providing access to a copy of the Policy;
  - (b) reminders of the need for compliance with the Policy; and
  - (c) providing updates or developments of the Policy,to those affected by the Policy.
- 4.3 It is the responsibility of all users to abide by the Policy.

### **5. Non-Compliance**

---

- 5.1 Depending on the nature of the inappropriate use of DE&T ICT systems, non-compliance with this Policy may constitute:
  - (i) a breach of employment obligations;
  - (ii) serious misconduct;
  - (iii) sexual harassment;
  - (iv) unlawful discrimination;
  - (v) a criminal offence;
  - (vi) a threat to the security of DE&T ICT systems;
  - (vii) an infringement of the privacy of staff and other persons; or
  - (viii) exposure to legal liability.
- 5.2 Non-compliance with this Policy will be regarded as a serious matter and appropriate action, including termination of employment, may be taken.

- 5.3 Where there is a reasonable belief that illegal activity may have occurred DE&T will report the suspected illegal activity to the police.

## **6. Business Purposes**

---

- 6.1 The DE&T ICT systems are tools to be used for DE&T purposes.
- 6.2 Use of DE&T ICT systems must –
- (a) be for DE&T purposes only, 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, ministerial orders or legislative requirements which apply to the user, for example, the Code of Conduct for the Victorian Public Sector, the *Teaching Service Act 1981* (Vic) and the *Public Administration Act 2004* (Vic).
- 6.3 Notwithstanding clause 6.2(a), users of DE&T ICT systems may use DE&T ICT systems for personal use provided the use is not excessive and does not breach this Policy. Users must not engage in excessive personal use of DE&T ICT systems during working hours. Users must not engage in excessive personal use of electronic communications and the Internet using DE&T networks outside working hours. A breach of either of these constitutes a failure to abide by this Policy.
- 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 and may constitute a criminal offence under the *Crimes Act 1958* (Vic) or other legislation.
- 6.6 Large downloads or transmissions should be minimised to ensure the performance of DE&T ICT systems for other users is not adversely affected. Where a user has caused DE&T to incur costs for excessive downloading of non-work related material in breach of this policy, DE&T may seek reimbursement or compensation from the user for all or part of these costs.

## **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 ICT systems.
- 7.2 Electronic communications created, sent or received by the users referred to in clause 1.2 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. All information produced on computer, including emails, may be accessible under the *Freedom of Information Act 1982* (Vic). Please note that Email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent.

## **8. Monitoring**

---

- 8.1 Use of DE&T ICT systems may be monitored by Authorised Persons.
- 8.2 From time to time, Authorised Persons may examine or monitor the records of DE&T ICT systems including for operational, maintenance, compliance, auditing, security or investigative purposes. For example, electronic communications and websites visited may be monitored. DE&T may investigate a complaint arising from the use of DE&T ICT systems.
- 8.3 Use of DE&T ICT systems is provided to users on condition that it is agreed that DE&T ICT systems are monitored in accordance with this Policy. Use of DE&T ICT systems constitutes consent to monitoring in accordance with this Policy.
- 8.4 If at any time there is a reasonable belief that DE&T ICT systems are being used in breach of this Policy, the principal or line manager of the person who is suspected of using DE&T ICT systems inappropriately may suspend a person's use of DE&T ICT systems and may require that the equipment being used by the person be secured by the principal or general manager while the suspected breach is being investigated.

## **9. Defamation**

---

- 9.1 DE&T ICT systems 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 widespread.

## 10. Copyright Infringement

---

- 10.1 The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video 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 and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing 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 DE&T ICT systems should 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 material

---

- 11.1 DE&T ICT systems must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and their employment may be terminated.
- 11.2 Illegal or unlawful use includes but is not limited to use of certain types of pornography (eg child pornography) under the *Crimes Act 1958* (Vic), offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic), defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking under the *Crimes Act 1958* (Vic), use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cyber Crime Act 2001* (Cth) or *Crimes Act 1958* (Vic) (as amended by the *Crimes (Property Damage and Computer Offences) Act 2003* (Vic)) or any other relevant legislation.
- 11.3 In particular, DE&T is an institution charged with the safety and education of children. Child pornography is abhorrent and represents the antithesis of DE&T's responsibilities to children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

## **12. Offensive or Inappropriate material**

---

- 12.1 Use of DE&T ICT systems must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.
- 12.2 The DE&T ICT systems must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually-oriented messages or images and messages that could constitute sexual harassment.
- 12.3 All users of DE&T ICT systems should be familiar with DE&T anti-discrimination, equal opportunity policies and harassment policies.
- 12.4 Users of DE&T ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their manager. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto DE&T ICT systems except where the material is required for the purposes of investigating a breach of this policy.

## **13. Confidentiality**

---

- 13.1 Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of DE&T ICT systems, 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.

## **14. Viruses**

---

- 14.1 Electronic communications are potential delivery systems for computer viruses. All data, programs and files which are downloaded electronically or attached to messages should be scanned by an anti-virus program before being launched, opened or accessed.
- 14.2 Viruses have the potential to seriously damage DE&T ICT systems. Do not open any downloaded files, 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.

## **15. Attribution**

---

- 15.1 There is always a risk of false attribution of breaches of this Policy. 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. 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 ICT systems that have been made available to them or leased to them for work purposes and all use of DE&T ICT systems performed with their user-ID. Users must maintain full supervision and physical control of DE&T ICT equipment, including notebook computers, at all times. User-IDs and passwords must be kept secure and confidential. User-IDs and passwords should not be disclosed to anyone, including disclosure to line managers or above. Users must not allow or facilitate unauthorised access to DE&T ICT systems through the disclosure or sharing of passwords or other information designed for security purposes.
- 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 and ‘Spam’**

---

- 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.
- 16.3 The use of electronic communications for sending unsolicited commercial electronic messages (‘Spam’) is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

## **17. Records Management**

---

- 17.1 Electronic Communications are public records and subject to the provisions of the *Public Records Act 1973* (Vic).
- 17.2 DE&T record management practices for management of email messages must comply with DE&T policies and guidelines on recordkeeping and management of electronic communications as amended from time to time.

- 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.
- 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 mail box. Messages for archive should be kept in separate archive files stored on the user's network home or shared drive.

## **18. Disclaimer**

---

- 18.1 All emails sent externally from DE&T's Edumail service will automatically have a disclaimer attached to them. The current 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.
- 18.3 School eMail systems must also append the same disclaimer (above) to messages sent externally from the School's Email service.

## **19. Complaints**

---

- 19.1 If you wish to make a complaint about an electronic communication which is offensive or inappropriate, raise it with your line manager, or, if your line manager is the cause of your complaint, raise it with your line manager's manager.

## **20. Breaches of this Policy**

---

- 20.1 Breaches of this Policy may be categorised using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. 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** – offences relating to child pornography are covered by the *Crimes Act 1958* (Vic) and the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Child pornography is defined in section 67A of the *Crimes Act 1958* (Vic) as:

“a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor engaging in sexual activity or depicted in an indecent sexual manner or context.”
- b. **Objectionable material** – offences relating to the exhibition, sale and other illegal acts relating to “objectionable films” and “objectionable publications” are covered by the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Such material has or would attract a classification of **X18+ (restricted)** or **RC (refused classification)** under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth).
- 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 non-criminal use of material that has or would attract a classification of **RC** under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). This covers any material that:

- a. depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;
- b. describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or

- c. promotes, incites or instructs in matters of crime or violence.

### **Category 3: Critical**

This category involves other types of offensive material. This covers any material that:

- a. Has or would attract a classification of **X18+** under Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). The material covered by this classification is only available for hire or sale in the ACT and Northern Territory, 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 and/or DE&T 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 employee's duties; and
- c. the use is more than insignificant.

## **21. Replacing previous policies**

---

- 21.1 This Policy replaces the "DE&T Acceptable Use Policy for Internet, Email and Other Electronic Communications."
- 21.2 This Policy does not replace the policy issued to schools titled "Safety Net, Internet Usage - Guidelines for Schools".

**Effective: 11 July 2006**