



ICT ACCEPTABLE USAGE POLICY STAFF

College council will review this policy every three years or as directed by DET

Date approved: October 2016

Date of next review: 2019

1. RATIONALE

- 1.1 The use of DET ICT resources carries with it responsibilities. Users must at all times remember that when using DET ICT resources, they are using ICT resources provided to them for business purposes.
- 1.2 The provision of DET ICT resources by DET is to improve and enhance learning and teaching, and conduct of the business and functions of DET. 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.
- 1.3 The process by which DET seeks to manage staff use of DET ICT resources is through the development and implementation of this Policy. The Policy must be followed whenever using DET ICT resources.

2. PURPOSE

- 2.1 The purpose of this Policy is to ensure that all use of Department of Education and Training (DET) Information, Communications and Technology (ICT) resources is legal, ethical and consistent with the aims, values and objectives of DET and its responsibilities to the students in its care. DET is an institution charged with the safety and education of children. It also has occupational health and safety obligations to employees and students and must comply with State and Federal anti-discrimination and sexual harassment laws. It is thus of paramount importance that its ICT resources are used appropriately and professionally at all times.
- 2.2 DET ICT resources must be properly and efficiently used. DET ICT resources are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

3. DEFINITION AND SCOPE

- 3.1 In this Policy:
 - i. an 'Authorised Person' means the Secretary, a Deputy Secretary, a Regional Director, an Assistant Regional Director, a Principal, General Manager Information Technology Division, Assistant General Manager, Information Technology Division, Manager, Risk Management (Information Technology Division), Manager Conduct & Ethics Branch, Officer, Conduct & Ethics Branch, or a person authorised by the Secretary of the Department of Education & Early Childhood Development;
 - ii. 'Copyright' does not include moral rights under the Copyright Act 1968 (Cth);
 - iii. 'DET' means the State of Victoria – Department of Education and Training;
 - iv. 'DET ICT resources' includes but is not limited to all DET networks, systems, software and hardware including DET Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, Ultranet, DET email systems, computer systems, software, servers, desktop computers, printers, scanners, portable computers, leased notebook computers, mobile phones, portable storage devices including digital cameras and USB memory sticks, hand held devices (for example, personal digital assistants or 'PDAs') and other ICT storage devices;

- v. 'Electronic Communications' means email, instant messaging and any other material sent electronically;
- vi. 'DET email systems' means eduMail and any other school-based email system established for the purposes of school-related communications. DET email systems are part of DET ICT resources;
- vii. 'Guidelines for Classification of Films and Computer Games' means the Guidelines for Classification of Films and Computer Games made under sub-section 12 of the Classification (Publications, Films and Computer Games) Act 1995 (Cth);
- viii. 'Malware' is an abbreviation of 'malicious software' and means software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware and trojans;
- ix. 'Peer-to-peer file sharing' means the sharing of files between systems on a P2P network. The 'peers' of a P2P network are computer systems connected to each other by the Internet. Files can be shared directly between computer systems on the network without the requirement of a central server. An example of illegal P2P file sharing is the sharing of copyrighted files without the authorisation of the copyright owner, for example copyrighted film and music files;
- x. 'Personal use' means all non-work related use, and includes internet usage and private emails;
- xi. 'Users' of DET ICT resources includes all employees, ie persons employed by the Secretary of DET under Part 2.4 of the Education and Training Reform Act 2006 (Vic), all persons employed by the Secretary of DET under the Public Administration Act 2004 (Vic), the Secretary of DET appointed under section 12 or 19 of the Public Administration Act 2004 (Vic), Ministerial officers and Ministers, working within DET, and all persons employed by school councils under Part 2.3 of the Education and Training Reform Act 2006 (Vic). It also includes all contractors and volunteers engaged by: DET, school councils, schools, regional offices or district offices who use DET ICT resources.

3.2 This Policy applies to all users of DET ICT resources regardless of work location and applies to all aspects of use of all DET ICT resources, for example:

Publishing and browsing on the internet;

- Downloading or accessing files from the internet or other electronic sources;
- Email;
- Electronic bulletins/notice boards;
- Electronic discussion/news groups;
- Weblogs ("blogs");
- Social networking;
- 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.

3.3 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.

4. RESPONSIBILITY

- 4.1** DET is responsible for ensuring 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, for example, on the DET website;
 - b) reminders of the need for compliance with the Policy; and
 - c) providing updates or developments of the Policy.
- 4.2** It is the responsibility of all users to abide by this Policy.

5. NON-COMPLIANCE

- 5.1** Depending on the nature of the inappropriate use of DET ICT resources, non-compliance with this Policy may constitute:
- a breach of employment obligations;
 - serious misconduct;
 - sexual harassment;
 - unlawful discrimination;
 - a criminal offence (see clause 11);
 - a threat to the security of DET ICT resources;
 - an infringement of the privacy of staff and other persons; or
 - 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 DET may report the suspected illegal activity to the police.

6. BUSINESS PURPOSES AND OTHER USE

- 6.1** Use of DET ICT resources must –
- a)** be for DET 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 resources 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 Education and Training Reform Act 2006 (Vic) and the Public Administration Act 2004 (Vic).
- 6.2** Notwithstanding clause 6.1(a), users of DET ICT resources may use DET ICT resources for personal use provided the use is not excessive and does not breach this Policy. Users must not engage in excessive personal use of DET ICT resources during working hours (refer to Clause 20, Category 4, for guidance). Users must not engage in excessive personal use of DET email systems or the internet using DET networks outside working hours. A breach of either of these constitutes a failure to abide by this Policy. In using DET ICT resources for personal use, users should be aware that the provisions that apply to access and monitoring of DET ICT resources apply to personal use as well.
- 6.3** Subject to limited personal use in accordance with clauses 6.2 and 20 -
- subscribing to mailing lists and other like services using DET ICT resources must be for DET purposes or professional development reasons only; and
 - social networking, on-line conferences, discussion groups or other similar services or tools using DET ICT resources must be relevant and used only for DET purposes or professional development activities. When using such tools, all DET ICT users must conduct themselves professionally and appropriately.
- 6.4** Provided that use is not unlawful, offensive or otherwise improper, users are allowed reasonable access to electronic communications using DET ICT resources to facilitate communication between employees and their representatives, which may include a union, on matters pertaining to the employer/employee relationship.

- 6.5** Large data downloads or transmissions should be minimised to ensure the performance of DET ICT resources for other users is not adversely affected. Where a user has caused DET to incur costs for excessive downloading of non-work related material in breach of this Policy, DET may seek reimbursement or compensation from the user for all or part of these costs.

7. DEPARTMENT PROPERTY

- 7.1** Electronic communications created, sent or received using DET email systems are the property of DET, and may be accessed by an Authorised Person in the case of an investigation, including in relation to investigations following a complaint or investigations into misconduct. 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. ACCESS AND MONITORING

- 8.1** DET ICT resources may be accessed or monitored by Authorised Persons at any time without notice to the user. This includes, but is not limited to, use of DET email systems and other electronic documents and records. However, Authorised Persons must have a valid reason for accessing or monitoring use of DET ICT resources in accordance with clause 8.3.
- 8.2** Before accessing or monitoring DET email systems an Authorised Person is required to contact the Manager, Risk Management (Information Technology Division) to inform him/her of the proposed access. A written log recording relevant details will be maintained by the DET Information Technology Division – Risk Management Team.
- 8.3** Authorised Persons may access or monitor the records of DET ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. For example, electronic communications, sent, received or forwarded using DET ICT resources, may be accessed and logs of websites visited using DET ICT resources may be generated, examined and monitored.
- 8.4** Authorised Persons may require the assistance of a systems administrator to gain access to records held within DET ICT resources such as electronic documents, communications or website logs of users. In such cases, the systems administrator will not be in breach of this Policy simply by reason of following the instructions of an Authorised Person.
- 8.5** If, at any time, a systems administrator discovers any inappropriate use of DET ICT resources, they must report their concerns to an Authorised Person.
- 8.6** Use of DET ICT resources constitutes consent to access and monitoring in accordance with this Policy.
- 8.7** If at any time there is a reasonable belief that DET ICT resources are being used in breach of this Policy, the principal or line manager of the person who is suspected of using DET ICT resources inappropriately may suspend a person's use of DET ICT resources and may require that the equipment being used by the person be secured by the principal or line manager while the suspected breach is being investigated.
- 8.8** Nothing in this Policy prevents the DET Information Technology Division or DET agents from monitoring DET ICT resources in order to support the functioning and performance of DET's information systems.

9. DEFAMATION

- 9.1** DET ICT resources 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 DET 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 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 DET liability, despite the belief that the use of such material was permitted.
- 10.2** DET supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.
- 10.3** All users of DET ICT resources should ensure they are familiar with the following publications issued by DET:
- a) DET Intellectual Property Policy and Principles;
 - b) DET Intellectual Property and Copyright Guidelines; and
 - c) Copyright Guidelines for Victorian Government Schools.

11. ILLEGAL USE AND MATERIAL

- 11.1** DET ICT resources 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** Certain inappropriate, unauthorised and non work-related use of DET ICT resources may constitute a criminal offence under the Crimes Act 1958 (Vic), for example, computer 'hacking' and the distribution of computer viruses.
- 11.3** 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, blackmail and threats 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.
- 11.4** In particular, DET is an institution charged with the safety and education of children. Child pornography represents the antithesis of DET'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 DET ICT resources 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** DET ICT resources 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 DET ICT resources should be familiar with DET anti-discrimination, equal opportunity and harassment policies.
- 12.4** Users of DET ICT resources who receive unsolicited offensive or inappropriate material electronically should delete it immediately. Offensive or inappropriate material received from people known to the receiver should be deleted immediately 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 DET ICT resources except where the material is required for the purposes of investigating a breach of this policy.

13. CONFIDENTIALITY AND PRIVACY

- 13.1** Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of DET ICT resources, 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.
- 13.2** In relation to communications relating to the disclosure of improper conduct either as part of an audit or as contemplated by the Whistle-blowers Protection Act 2001 (Vic), it is advised that personal, not DET, email accounts or other means of communication are used to report this information to maintain confidentiality.
- 13.3** DET will handle any personal information collected through the use of DET ICT resources in accordance with the Information Privacy Act 2000 (Vic).
- 13.4** DET will not disclose the content of electronic communications created, sent or received using DET ICT resources to third parties outside of DET unless that disclosure is required for the purposes of a DET investigation, a police investigation or for other legal, investigative, audit or compliance reasons or in other circumstances where that disclosure does not contravene the Information Privacy Act 2000 (Vic).

14. MALWARE

- 14.1** Electronic and web communications are potential delivery systems for computer malware. 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** Malware has the potential to seriously damage DET ICT resources. Do not open any attachments or click on any links embedded in an email unless you have confidence in the identity of the sender.

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 DET ICT resources that have been made available to them or leased to them for work purposes and all use of DET ICT resources performed with their User ID. Users must maintain full supervision and physical control of DET ICT resources, including notebook computers, at all times. User ID's and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to DET ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.
- 15.3** Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.

16. MASS DISTRIBUTION AND 'SPAM'

- 16.1** The use of DET ICT resources 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 DET 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 DET record management practices for management of email messages must comply with DET 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 DET's eduMail service will automatically have a disclaimer attached to them.
- 18.2 The disclaimer must not be altered or interfered with in any way. The use of the disclaimer may not necessarily prevent DET or the sender of the email from being held liable for its contents.
- 18.3 School email systems must also append the same disclaimer to messages sent externally from the school's email service.

19. COMPLAINTS

- 19.1 If you wish to make a complaint or report about inappropriate use of DET ICT resources raise it with your principal or line manager, or, if your principal or line manager is the cause of your complaint, raise it with their manager.
- 19.2 DET may investigate complaints arising from the use of DET ICT resources or complaints arising from the application of this policy in accordance with DET Guidelines for Managing Complaints, Misconduct and Unsatisfactory Performance.

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);
- 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 a 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 DET 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);
- b) it adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties;
- c) the use is more than insignificant.

21. OTHER POLICIES

- 21.1 This Policy replaces the 'Acceptable Use Policy for DET Information Communications and Technology (ICT) Systems'.
- 21.2 This Policy operates in conjunction with DET's 'Terms of Service' for use of the Ultranet.
- 21.3 This Policy operates in conjunction with DET's 'Information and Communication Technology Security Policy'.
- 21.4 This Policy operates in conjunction with 'Notebook Computers Terms and Conditions Licence Agreement' or any other agreements entered into as part of the Notebook for Teachers and Principals Program.