VICTORIA State Government | Education and Training

Human Resources

Acceptable Use -

Information and Communications Technology Resources

Last updated 11 July 2018

CONTENTS

Overview

This Guide outlines the policy regarding the acceptable use of the Information and Communications Technology (ICT) resources of the Department of Education and Training (the Department).

The Department is responsible for ensuring the use of Department ICT resources is legal, ethical and consistent with the aims, values and objectives of the Department and its responsibilities to employees, students and other ICT users.

All users of Department ICT resources are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others and operate within the laws of the State and Commonwealth, including anti-discrimination and sexual harassment laws and the rules and policies of the Department, including occupational health and safety obligations to employees and students.

Department ICT resources should not be used for inappropriate or improper activities. This includes: pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, bullying, privacy violations and illegal activity, including illegal peer-to-peer file sharing. The audience of an electronic message may be unexpected and widespread and users should be mindful of this when using Department ICT resources.

Department ICT resources are provided to improve and enhance learning and teaching, and for the conduct of the business and functions of the Department. Using information technology, accessing information, and communicating electronically can be cost-effective, timely and efficient. Users are expected to use and manage these resources in an appropriate manner and in accordance with this policy. As part of ensuring users are aware of this policy, the following will occur:

- Users will be provided access to this policy, on HRWeb
- Users will be reminded of the need for compliance with the policy
- Users will be provided notification of updates or developments to the policy.

Scope

This policy applies to all users of Department ICT resources, as defined below, located at corporate offices and schools, and in private homes or at any other location. This policy applies to all use of Department ICT resources, including, but not limited to:

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

Definitions

Authorised person For the purpose of this policy, includes:

The Secretary, a Deputy Secretary, an Assistant Deputy Secretary, a Regional Director, a regional Executive Director, a School Principal, the Executive Director People Division, the Chief Information Officer (CIO) or equivalent roles (or delegate).

The Manager of the Employee Conduct Branch or the equivalent branch, or an officer of the Employee Conduct Branch authorised by the manager.

Any other person authorised by the Secretary to the Department of Education and Training.

Department email systems eduMail and any other school or Department email system used for the purpose of school related or other Department electronic communications. Department email systems are part of Department ICT resources.

Department ICT resources Includes but is not limited to all networks, systems, software and hardware including local area networks, wide area networks, wireless networks, intranets, Department email systems, computer systems, software, servers, desktop computers, printers, scanners, personal computers (desktops, notebooks and tablets), mobile phones, portable storage devices including digital cameras and USB memory sticks, hand held devices and other ICT storage devices.

Electronic communications Includes email, instant messaging, virtual conferencing, social media and any other material sent electronically.

Malware Malicious software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware and trojans.

Peer-to-peer file sharing The sharing of files between systems on a peer-to-peer (P2P) network. Files can be shared 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, such as copyrighted film, book and music files.

Personal use All non-work related use of Department ICT resources including internet usage, social networking and private emails.

Phishing Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Ransomware Ransomware is a type of malicious software that threatens to publish the victim's data or block access to it unless a ransom is paid.

Spam Unsolicited commercial electronic messages sent over the internet.

User/s Any person using Department ICT resources.

Vishing Vishing is a form of phishing that uses the phone system or voice over IP (VoIP) technologies. The user may receive an email, a phone message, or even a text encouraging them to call a phone number due to some discrepancy. If they call, an automated recording prompts them to provide detailed information to verify their account such as credit card number, expiration date, birthdate.

Whaling Whaling is a type of phishing that targets high-profile users such as corporate executives, politicians and celebrities. Whaling emails and websites are highly customized and personalised, often incorporating the target's name, job title or other relevant information gleaned from a variety of sources.

Non-compliance

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken, which may include termination of employment.

Depending on the nature of the inappropriate use of Department ICT resources, non-compliance with this policy may constitute:

- A breach of employment obligations
- A criminal offence
- A threat to the security of Department ICT resources and information
- An infringement of the privacy of staff and other persons
- Exposure to legal liability
- Serious misconduct
- Sexual harassment
- Unlawful discrimination.

Where there is a reasonable belief that illegal activity may have occurred, this may be reported to the police.

Breaches of this Policy

Breaches of this policy may fall into one of the following categories, described in detail in the below table all of which brings, or has the potential to bring, the employee and/or the Department into disrepute:

- Category 1: Illegal - criminal use of material
- Category 2: Extreme - non-criminal use of material
- Category 3: Critical - offensive material.
- Category 4: Serious

Category	Description
1 Illegal	This category includes but is not limited to: • Child abuse material offences relating to child pornography covered by the *Crimes Act 1958* (Vic).'Child abuse material' is defined in section 51A of the *Crimes Act 1958* (Vic). • Objectionable material - offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' 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 2012, Guidelines for the Classification of Computer Games 2012* or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). • Reckless or deliberate copyright infringement. • Any other material or activity that involves or is in furtherance of a breach of criminal law.
2 Extreme	This category includes: • non-criminal use of material that has or may attract a classification of RC or X18+ under the *Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012* or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). This includes any material that: ○ 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 ○ Describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not) ○ Promotes, incites or instructs in matters of crime or violence ○ Includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults.
3 Critical	This category includes other types of restricted or offensive material, covering any material that: • Has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995 (Cth)*. Material may contain sex scenes and drug use that are high in impact. • Includes sexualised nudity • Involves racial or religious vilification • Is unlawfully discriminatory • Is defamatory • Involves sexual harassment or bullying
4 Serious	This category includes any use which is offensive or otherwise improper.

The categories do not cover all possible breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.

Use of Department ICT resources

BUSINESS PURPOSES

Department ICT resources are provided to users for business purposes. Other than limited personal use, Department ICT resources must be:

- Used for business purposes, or where authorised or required by law, or with the express permission of an Authorised Person
- Used like other business resources and users must comply with any codes of conduct, ministerial orders or legislative requirements that 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)*.

Users are allowed reasonable access to electronic communications using Department ICT resources to facilitate communication between employees and their representatives, provided that use is not unlawful, offensive or otherwise improper. This may include a union on matters pertaining to the employer/employee relationship.

Large data downloads or transmissions should be minimised to ensure the performance of Department ICT resources for other users is not adversely affected.

PERSONAL USE

Users may use Department ICT resources for personal reasons provided the use is not excessive and does not breach this policy.

Excessive personal use during working hours covers personal use which satisfies the following criteria:

- It occurs during normal working hours (but excluding an employee's lunch or other official breaks);
- It adversely affects, or could reasonably be expected to adversely affect, the performance of the employee's duties; and
- The use is not insignificant.

The Department may seek reimbursement or compensation from a user for all or part of any costs where the user has caused the Department to incur costs due to excessive downloading of non-work related material in breach of this policy.

Subject to limited personal use, social networking, on-line conferences, discussion groups or other similar services or tools using Department ICT resources must be relevant and used only for Department purposes or professional development activities. Users must conduct themselves professionally and appropriately when using such tools.

Unless otherwise approved, for ICT security reasons Department email addresses should not be used to subscribe to private subscriptions and other like services (e.g. on line ticket services, bill payments) and should never be used as "recovery email' addresses for any other services. Subscribing to mailing lists and other like services using Department ICT resources must be for Department purposes or professional development reasons only and a different password must be used for all such purposes.

Users should be aware that the provisions applying to access and monitoring of Department ICT resources also apply to personal use.

DEFAMATION

Department 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 Department liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

COPYRIGHT INFRINGEMENT

The copyright material of third parties must not be used without authorisation. This includes software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text and downloaded information.

The ability to forward, distribute and share electronic messages, attachments and files greatly increases the risk of copyright infringement. Copying material to electronic storage, or printing, distributing or sharing copyright material by electronic means may give rise to personal and/or Department liability, despite the belief that the use of such material was permitted.

Users of Department ICT resources should be familiar with any relevant intellectual property and copyright guidelines issued by the Department.

For the avoidance of doubt, “copyright” does not include moral rights under the *Copyright Act 1968 (Cth)*.

ILLEGAL USE AND MATERIAL

Department ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender may be referred to the police or other relevant authority and their employment may be terminated.

Certain inappropriate, unauthorised and non work-related use of Department ICT resources may constitute a criminal offence under the *Crimes Act 1958* (Vic). Examples include computer ‘hacking’, unauthorised release of data, Department material or leaking of information or documents and the distribution of malware.

Illegal or unlawful use includes but is not limited to:

- Use of certain types of pornography under the *Crimes Act 1958* (Vic), such as child pornography
- Offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic)
- Defamatory material
- Material that could constitute racial or religious vilification, or unlawfully discriminatory material
- Stalking
- Blackmail and threats under the *Crimes Act 1958* (Vic)
- Use that breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cybercrime Act 2001* (Cth) or *Crimes Act 1958* (Vic).
- Breaches under any other relevant legislation.

In particular, child abuse materials represents the antithesis of Department responsibilities with regard to the safety and education of children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

OFFENSIVE OR INAPPROPRIATE MATERIAL

Use of Department ICT resources must be appropriate to a workplace environment and aligned to Department Values. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

Department 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.

All users of Department ICT resources should be familiar with Department policies including: anti-discrimination, human rights, equal opportunity and bullying and harassment.

Users of Department ICT resources who receive unsolicited, offensive or inappropriate material electronically should delete it immediately and may choose to notify their principal or immediate manager of such instances. Where the sender of this material is known to the user, the user should notify the sender to refrain from sending such material again.

Offensive or inappropriate material must not be forwarded internally or externally, or saved onto Department ICT resources, except where the material is required for the purposes of investigating a breach of Department policies.

MALWARE

Electronic and web communications are potential delivery systems for computer malware. An anti-virus and threat protection program should scan all data, programs and files downloaded electronically or attached to messages before being launched, opened, accessed or sent.

Malware has the potential to seriously damage Department ICT resources and lead to a breach of privacy legislation. Users should not open any attachments or click on any links embedded in an email unless they have confidence in the identity of the sender.

SOCIAL ENGINEERING

Social engineering is (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Phishing, Vishing and Whaling and other forms of social engineering are used to obtain information from users that could result in unauthorised access to Department ICT resources, or to fraudulently obtain money from the Department.

ATTRIBUTION

There is always a risk that an employee may be in breach of this policy due to false attribution. 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. Users should inform their immediate manager or principal if they believe an electronic communication has been intercepted or modified.

Users are accountable for all use of Department ICT resources that have been made available to them for work purposes and for all use of Department ICT resources performed with their user identification. Users must maintain full supervision and physical control of Department ICT resources at all times, including mobile phones, tablets and notebook computers.

User identification and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to Department ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.

MASS DISTRIBUTION AND SPAM

The use of Department ICT resources for sending ‘junk mail’, for-profit messages, or chain letters is strictly prohibited.

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).

Mass electronic communications should only be sent in accordance with normal Department procedures.

Confidentiality and Privacy

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of Department ICT resources, 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.

To ensure their confidentiality is maintained, employees are advised to use personal, rather than Department email accounts when disclosing improper conduct, either as part of an audit or as contemplated by the *Protected Disclosure Act 2012* (Vic).

The Department will handle any personal information collected through the use of Department ICT resources in accordance with the *Privacy and Data Protection Act 2014* (Vic).

The Department will not disclose the content of electronic communications created, sent or received using Department ICT resources to third parties outside of the Department unless that disclosure is required for the purposes of:

- A Department investigation
- A police investigation,
- For other legal, investigative, audit or compliance reasons.

In other circumstances, disclosure should not contravene the *Privacy and Data Protection Act 2014* (Vic).

Department Property

Electronic communications created, sent or received using Department email systems are the property of the Department and may be accessed by an Authorised Person or their delegate in the case of an investigation. This includes 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 users' computers, including emails, may be accessible under the *Freedom of Information Act 1982* (Vic).

Email messages may be retrieved from back-up systems.

Email Disclaimer

All emails sent externally from the eduMail service will automatically have a disclaimer attached to them.

The use of the email disclaimer may not necessarily prevent the Department or the sender of the email from being held liable for its contents.

School email systems must also append the same disclaimer to messages sent externally from the school's email service.

Access and Monitoring

Authorised Persons may access or monitor Department ICT resources at any time without notice to the user. This includes, but is not limited to, use of Department email systems, and other electronic documents and records and applies to the use of Department ICT resources for personal use. However, Authorised Persons must have a valid reason for accessing or monitoring the use of Department ICT resources and are required to maintain a log recording relevant details of the access and monitoring activity.

Authorised Persons are required to inform the Chief Information Officer (CIO), Information Management and Technology Division (IMTD) before accessing or monitoring Department ICT resources.

Authorised Persons may access or monitor the records of Department ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. Electronic communications that have been sent, received or forwarded using Department ICT resources, may be accessed and logs of websites visited using Department ICT resources may be generated, examined and monitored.

Authorised Persons may require assistance of a systems administrator to gain access to records held within Department 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 by reason of following the instructions of an Authorised Person.

If a systems administrator becomes aware of any inappropriate use of Department ICT resources, they must report their concerns to an Authorised Person.

If there is a reasonable belief that Department ICT resources are being used in breach of this policy, the principal or immediate manager of the person who is suspected of inappropriate use may secure the equipment while the suspected breach is being investigated.

The principal or immediate manager may also request the CIO to suspend a person's use of Department ICT resources.

Nothing in this policy prevents IMTD or Department agents from monitoring Department ICT resources in the normal course of their duties.

Records Management

Electronic communications are public records and subject to the provisions of the *Public Records Act 1973* (Vic).

Department record management practices must comply with Department policies and guidelines on records management and management of electronic communications, as amended from time to time. Department records may either:

- Have no retention requirement and be destroyed as soon as they are no longer required for administrative purposes.
- Be retained as a temporary record by the Department and then destroyed when the retention period designated by the Public Record Office Victoria (PROV) is complete.
- Be retained as a permanent record by the Department then, when no longer required for administrative use, transferred to PROV.

Complaints

If an employee has a complaint or report of inappropriate use of Department ICT resources, they should lodge it with the immediate manager or principal of the person who the complaint is about. If the complaint is about the employee's immediate manager or principal, they should raise it with the manager above.

Complaints arising from the use of Department ICT resources or complaints arising from the application of this policy may be investigated in accordance with Department guidelines for managing complaints, misconduct and unsatisfactory performance for the teaching service or the public service, as appropriate.

'SPEAK-UP' SERVICE

Employees, contractors, and consultants are encouraged to report inappropriate conduct. If an employee has any known or suspected concerns about the appropriateness of someone's ICT use by way of an unlawful act or omission, unethical behavior, or breach of the policy, and is unable to raise it with an appropriate manager, disclosures can be made through a third-party service provider. Disclosures will be treated confidentially.

- Hotline service: 1800 633 462
- Email: educationspeakup@risqgroup.com
- Web portal: www.risqgroup/dms/educationspeakup

Further Assistance

Further information, advice or assistance on any matters related to acceptable use of Department ICT resources is available by:

- accessing the A-Z topic list on HRWeb;
- using the related topics list; or
- contacting the Information Management and Technology Division on 1800 641 943 or the Employee Conduct Branch on 9637 2594