Introduction

This policy outlines appropriate usage of Department of Premier & Cabinet (DPC) Information, Communications and Technology (ICT) resources. ICT resources include but are not limited to: networks, email, smartphones, tablets, laptops, Wi-Fi, internet/CRM systems, TRIM, CBM and all other systems. Inappropriate use can expose DPC to risks, including security attacks, legal liability and network systems/services being compromised.

Public servants are required to demonstrate the Victorian Public Sector (VPS) values; including to act impartially and with integrity, to be accountable for their behaviour and to provide a responsive service. The VPS Code of Conduct sets the standards of behaviour for all Victorian public sector employees.

All employees, contractors, consultants, temporary/agency employees and other workers within DPC must:

- Securely handle departmental information
- Foster a productive workplace that is safe and free of discrimination and harassment
- Responsibly use government resources and equipment.

Every attempt is made to ensure the security of DPC's ICT resources; however, users must be aware that this security is not always guaranteed, particularly when communicating with an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication. They must treat the department's information as confidential and must comply with this policy, all related guidelines and other policies and legislations.

Purpose

DPC is committed to preserving the availability, confidentiality and integrity of the physical and information assets of the department. This policy has been issued by DPC for the purposes of:

- Meeting regulatory and legislative requirements regarding the use and handling of information
- Ensuring all breaches of information security, actual or suspected, are reported
- Aligning information security with the needs of the department (determined via DPC risk management)
- Ensuring DPC's business requirements for the availability of information and systems are met
- Protecting information on ICT systems from unauthorised access
- Safeguarding the confidentiality of information on DPC's ICT systems.

Scope

This policy applies to employees, contractors, consultants, temporary/agency employees and other workers within DPC, including all personnel affiliated with third parties working at DPC offices. This policy relates to all equipment, systems and, more broadly, intellectual property and information that is owned by DPC. This policy covers all DPC information, whether it is accessed via ICT resources or other means.

The department's information is classified in a number of ways and defined by DPC's guidelines and processes. Examples of confidential information include but are not limited to briefs, correspondence, policy advice, documentation around corporate strategies and other data. All people covered by this policy must take all necessary steps to prevent unauthorised access to this information.

This policy applies to the use of all DPC ICT resources including but not limited to the following activities:

- Browsing on the internet (either via desktop or Wi-Fi) and downloading/accessing files from the internet
- Emailing and instant messaging
- Video conferencing and weblogs ('blogs')
- Copying, saving, distributing, storing files and printing material

Definitions

CRM: (Customer Relationship Management system) managing DPC's interactions. It uses technology to organise, automate and synchronise business processes for information, customer service and technical support

TRIM: DPC's Central Repository for Information

CBM: Connect Brief Management is DPC's Brief and Correspondence Tracking System

ICT: Information, Communications and Technology

SEC STD: Security Standard

SOE: Standard Operating Environment is DPC's operating system and associated software

IT: Information Technology

IM: Information Management

Principles

DPC is committed to maintaining a balance between personal use and privacy for users while protecting the interests of DPC.

DPC ensures any person working at DPC treats all information they access and produce as confidential and that all information is managed appropriately in line with relevant policies and legislation

- DPC ensures efficient management of DPC's networks, computers and smartphones in relation to internet, email, security and more broadly intellectual property and information
- DPC provides clear guidance on acceptable and prohibited use of IT and IM at DPC
- DPC recognises that social media tools and social networking websites can benefit users in relation to their work in DPC and to also communicate set guidelines for appropriate use as a DPC employee.

Responsibilities

Information Management & Technology (IMT) Branch is responsible for creating guidelines concerning personal use of systems. If there is any uncertainty, employees should consult their manager or contact the IMT Branch for clarification. Please read carefully the following list of responsibilities that apply to all people covered by this policy.

- Employees must demonstrate sound judgment regarding the reasonableness of personal use. Personal use is acceptable provided it does not interfere with work productivity or breach any of the expressed requirements set out in this policy and its related guidelines
- DPC employees must keep passwords secure and must not share accounts
- All mobile devices (i.e. notebooks, laptops, iPads, iPhones etc) must be secured or locked away when unattended to avoid theft. This also extends to locking your computer screen
- Information accessed and produced by DPC employees is owned by the State of Victoria. Such information includes material that has been removed from the system (i.e. burned to CD, transferred to a USB drive, etc.)
- Information on portable storage devices can have a greater element of risk and, as such, needs to be managed more carefully by employees who use these devices
- All equipment connected to the DPC network, either personally or departmentally owned, will be scanned and protected from viruses. Employees must use appropriate caution when opening email attachments, which may contain viruses, Trojans, etc. DPC employees are not required to identify themselves as a current or former employee of DPC on social media sites, but are expected to behave appropriately and consistently with DPC policies. The departmental preference is that DPC employees, contractors, consultants, temporary/agency employees or any other workers within DPC (current or former); do not identify themselves as such on social media. Where employees do identify themselves as a DPC staff member they must include appropriate disclaimers that their contributions do not represent the view of the department or the Victorian Government

- All staff must keep in mind that it might be possible for an unauthorised person to gain access to the department's premises. Therefore, all business documents which include confidential papers, works in progress and drafts, should be securely stored away when you are not at your desk.

. Unacceptable use of DPC's ICT resources includes but is not limited to:

- Engagement in any activity that is illegal while using DPC-owned resources
- Conducting private commercial activity on internet or email
- Downloading any applications <u>not</u> part of the SOE or supported products listed outside the SOE
- Installing any copyrighted software for which DPC does not have an active licence (staff are obligated to find out whether a licence exists and if not, are responsible for obtaining accordingly)
- Deliberately introducing malicious programs into the network or domain (e.g. viruses, worms, Trojans, etc.)
- Revealing account passwords to others or allowing others to use their account. This includes family and other household members when working from home using personal or DPC resources.
- Family using a DPC device
- Using a DPC asset to actively engage in procuring or transmitting material that is in violation of sexual harassment and/or workplace laws
- Making fraudulent statements or offers of service originating from any DPC account
- Accessing data not intended for your use or attempting to log on to a server or account you are not authorised to access
- Creating a network disruption by conducting activities that do not align with our Information Security Policy (i.e.: network sniffing, packet spoofing and other actions that maliciously attack information)
- Providing information about DPC employees to external parties without appropriate consent
- Sending unsolicited email messages, including material that violates copyright, the sending of "junk mail" and "chain letters", sexually orientated messages or images or other advertising material to individuals who did not specifically request such material (e.g. email spam)
- Any form of harassment via email, telephone or other electronic means
- Gaining access or attempting to access gambling sites or sites portraying text, graphics, audio or video of an offensive, pornographic or illegal nature or directing another to such material on the internet or elsewhere
- Gaining unauthorised access to websites or databases and altering their content
- Simultaneously sending to several DPC users an email that contains a large file attachment (over 20MB) and whose memory requirements may reasonably be expected to significantly degrade network capacity
- Downloading files more than 20MB from the internet or opening non-work-related email attachments whose memory requirements may reasonably be expected to significantly degrade network capacity
- Exceeding designated data limit of 1GB per month. (Note: a data usage report is sent to Managers for review)
- Commenting via social media on DPC or its policies or revealing official information that is not publicly available
- Performing any activity that breaches any DPC ICT related policies

Reporting and Investigation

DPC has processes and systems to monitor the department's level of information security. While these processes and systems provide a comprehensive level of privacy, users need to be aware that the data and information they create while employed by DPC remains the property of the department at all times. For security and network maintenance purposes, authorised individuals within DPC reserve the right to monitor equipment, systems and network traffic at any time and may therefore, audit networks and systems on a regular basis to ensure compliance with this policy.

All internet usage on a mobile device is recorded against the unique Internet Protocol (IP) address of the hardware. When using the internet, the web address of any site visited, date and time it was visited, and duration of any visit is logged. DPC can carry out a random compliance audit at any time. A web filtering service provides both a filtering and reporting capability. The filtering service blocks access to websites categorised as inappropriate and also provides a way of monitoring internet use.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, in accordance with DPC's misconduct or relevant HR policies

Relevant Legislation and Policies

In using DPC information, the conduct of all employees is subject to the terms of this policy any other applicable law, policies and/or procedures, including the following:

- DPC's Social Media Policy – Located in TRIM (D11/219587)
- DPC's Information Security Policy – Located in TRIM (D12/10802)
- The Code of Conduct for Victorian Public Sector Employees
- The Equal Opportunity Act 2010 (VIC)
- The Occupational Health and Safety Act 2004 (VIC)
- Disability Discrimination Act 1992
- Sex Discrimination Act 1984
- Racial Discrimination Act 1975
- Racial and Religious Tolerance Act 2001
- Age Discrimination Act 2004
- Public Records Act 1973
- Information Privacy Act 2000
- Spam Act 2003

Contact

Name:	Chief Information Officer, DPC
Branch name:	Information Management & Technology
Branch contact details:	3/1 Macarthur Place, East Melbourne - 965 15715 Business Technology

Policy management

TITLE AND VERSION NO.	V3.0
POLICY OWNER/BRANCH	Information Management & Technology
DATE OF EXECUTIVE APPROVAL	March 2013 – Secretary, DPC
EFFECTIVE DATE	March 2013
NEXT REVIEW DATE	September 2016

End of policy.