

USE OF TECHNOLOGY

Contents

Authority and Application	1
Overview	1
Relevant provisions of the VPS Agreement.....	2
Guidance Information.....	2
1. Definitions.....	2
2. Employee use of ICT Resources	2
3. Inappropriate use	2
4. Monitoring and surveillance	3
5. Privacy.....	4
6. Security	4
Further Information.....	4
Related policies or documents.....	4

Authority and Application

The *Victorian Public Service Enterprise Agreement 2020* (**Agreement**) applies to Victorian Public Service Departments and Agencies (**Employers**) and their Employees covered by the Agreement.

Overview

Use of technology is essential for performing work in a modern workplace. This policy provides guiding principles on the use of information and communication technology (**ICT**) resources, including reasonable personal use of those resources and accessing resources on a device provided by an Employee. The Code of Conduct for Victorian Public Sector Employees 2015 (**Code of Conduct**), the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)* impose obligations on the provision, maintenance and use of technology. This policy summarises those obligations and provides guidance for consistent practices across the Victorian Public Service.

The Employer will have their own policies about the use of ICT Resources. This Policy should be read in conjunction with those Employer policies.

Relevant provisions of the VPS Agreement

Guidance Information

1. Definitions

- 1.1. **ICT Resources** means all information and communication technology resources owned, controlled or provided by the Employer and used to undertake its operations, including all networks, systems, applications, software and hardware. An ICT Device provided by the Employer is also an ICT Resource.
- 1.2. **ICT Device** means a piece of hardware used to access ICT Resources, including desktop computers, mobile phones, laptop computers, tablets and security tokens. The device may be provided by the Employer or provided by an Employee.
- 1.3. **BYO Device** means an ICT Device that is provided by an Employee.
- 1.4. **Privacy Principles** means:
 - 1.4.1. the Information Privacy Principles in the *Privacy and Data Protection Act 2014* (Vic); and
 - 1.4.2. the Health Privacy Principles in the *Health Records Act 2001* (Vic).

2. Employee use of ICT Resources

- 2.1. There are three common circumstances in which an Employee may use ICT Resources:
 - 2.1.1. Using an ICT Device provided by the Employer for a work-related purpose
 - 2.1.2. Using an ICT Device provided by the Employer for a personal purpose
 - 2.1.3. Using a BYO Device to access ICT Resources.
- 2.2. This policy applies to Employee use of ICT Resources at the Employer's office/s or any other location.
- 2.3. ICT Resources, including ICT Devices provided by the Employer, are provided by the Employer for work-related purposes. It is common practice for Employers to permit reasonable personal use of ICT Resources. It is recommended that Employer policies about the use of ICT Resources permit such reasonable personal use.
- 2.4. Where the Employer permits reasonable personal use of ICT Resources, its policies about the use of ICT Resources should provide guidance on the type and amount of personal use that is reasonable. Employer policies about the use of ICT Resources may provide for circumstances where it may recover the cost of unreasonable personal use from an Employee.
- 2.5. The Employer must reimburse Employees for use of their personal mobile phone or home phone if such use meets the requirements of clause 36.3 of the Agreement (including that that use has been prior approved by the Employer – see clause 36.3(b)). Employer policies about use of ICT Resources may provide for circumstances in which the Employer will otherwise reimburse the Employee for use of a BYO Device for work-related purposes.
- 2.6. The Employer must allow reasonable access to ICT Resources to facilitate communication between employee/s and/or their Union in accordance with clause 77.2(c) of the Agreement. Employees must ensure that such communications are reasonable, not offensive or improper.

3. Inappropriate use

- 3.1. Employees are responsible for ensuring their use of ICT Resources is appropriate. Inappropriate use of ICT Resources may be misconduct and dealt with under the Misconduct Common Policy and clause 25 of the Agreement. Inappropriate use can include use of ICT Resources for a work-related or personal purpose.
- 3.2. Inappropriate use of ICT Resources includes, but is not limited to, use that is inconsistent with the VPS Code of Conduct, the values in the *Public Administration Act 2004* or a policy of the Employer.
- 3.3. Inappropriate use includes criminal and unlawful use of ICT Resources:
 - 3.3.1. Criminal use of ICT Resources is any use that is, or is part of, a criminal offence under a State or Commonwealth law
 - 3.3.2. Unlawful use of ICT Resources is any use that contravenes a law, other than a criminal law, of the State or the Commonwealth.
- 3.4. For the avoidance of doubt, employee use of ICT Resources to perpetrate sexual harassment or family violence constitutes an inappropriate use.
- 3.5. Contravention of intellectual property laws is a form of unlawful use of ICT Resources, including unauthorised reproduction of copyright materials.
- 3.6. Employer policies about the use of ICT Resources may specify types of inappropriate use that are or are not relevant to its operations. Where an employee uses social media, for a work-related or personal purpose, the Employee must also comply with the Employer's social media policy (if any).
- 3.7. The Employer will report inappropriate use of ICT Resources to a law enforcement agency, regulator or other body, where a law of the State or the Commonwealth requires it to do so. For example, some use of ICT Resources may be reportable conduct under Part 5A of the *Child Wellbeing and Safety Act 2005* (Vic). Where a matter is classified as a protected disclosure, parties must also comply with their obligations under the *Protected Disclosures Act 2012* (Vic).
- 3.8. The Employer may report other suspected criminal or unlawful use of ICT Resources to a law enforcement agency, regulator or other body. It is not necessary for the Employer to be satisfied that a contravention or criminal offence has occurred before making the report.
- 3.9. Employees that become aware of, or have a reasonable suspicion, of inappropriate use, including criminal or unlawful use, of ICT Resources should report it to their Employer. Inappropriate use may constitute unethical behaviour that Employees are expected to report to an appropriate authority in accordance with clause 3.6 of the Code of Conduct.
- 3.10. Where the Employer has a reasonable belief that an Employee's use of ICT Resources is inappropriate, the Employer may suspend the Employee's access to ICT Resources including, but not limited to, whilst an investigation into the suspected inappropriate use is occurring.

4. Monitoring and surveillance

- 4.1. The Employer may conduct monitoring and surveillance of their ICT Resources for any lawful purpose. The Employer should ensure any monitoring and surveillance activity is not an offence under the *Surveillance Devices Act 1999* (Vic).
- 4.2. Employer policies about the use of ICT Resources may also provide information about:
 - 4.2.1. ICT Resources that require an Employee's consent before being accessed for monitoring or surveillance (eg email, restricted calendars, storage drives);
 - 4.2.2. senior personnel that have authority to access all ICT Resources without consent from an Employee (eg the Chief Information Officer or their nominee);

4.2.3. circumstances in which information obtained from monitoring and surveillance activities may be disclosed; and

4.2.4. monitoring and surveillance of a BYO Device, including the extent to which the Employer has access to and will monitor personal use of the BYO Device.

5. Privacy

- 5.1. Section 13 of the *Charter of Human Rights and Responsibilities 2006* (Vic) recognises a person's right to not have their privacy unlawfully or arbitrarily interfered with. The Employer is required to act in a way that is not incompatible with human rights.
- 5.2. The Employer must comply with their obligations under the *Privacy and Data Protection Act 2014* (Vic) and *Health Records Act 2001* (Vic), including the Information Privacy Principles.
- 5.3. ICT Resources are used to collect, use, disclose, access, correct and handle information, including personal information and health information. The Employer will ensure their policies about the use of ICT Resources are consistent with their privacy policy. Employees will not use ICT Resources to collect, use, disclose, access, correct or handle personal information or health information for a purpose that is inconsistent with the Privacy Principles and the Employer's privacy policy.
- 5.4. Information gathered from monitoring and surveillance of ICT Resources may be personal information or health information and must be collected, used, disclosed, accessed, corrected and handled in accordance with the Privacy Principles.
- 5.5. The Employer may allow a third-party, including CenITex, or other Government Service Provider to access its ICT Resources for monitoring, surveillance, maintenance or other service delivery reasons. Third parties that have access to personal and health information will be required to meet the same obligations as the Employer.

6. Security

- 6.1. The Employer may require Employees to follow conditions of use that enhance the security and integrity of ICT Resources. The Employer must ensure Employees are aware of the conditions of use, including how this may affect their personal use of a BYO Device.
- 6.2. Employees must ensure they comply with the conditions of use of ICT Resources. If an Employee believes their use of ICT Resources may have compromised the security and integrity of those resources, they should report it to the Employer as soon as possible.

Further Information

Employees should refer to their Department or Agency's intranet for information on procedural requirements, systems and approval delegations.

For further information and advice please contact your local Human Resources, People and Culture or Information, Communication and Technology Unit (or equivalent).

Related policies or documents

Code of Conduct for Victorian Public Sector Employees

<https://vpssc.vic.gov.au/html-resources/code-of-conduct-for-victorian-public-sector-employees/>

Privacy and Data Protection Act 2014 (Vic)

[http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/6BF03254A893AFC4CA258314001B4CF2/\\$FILE/14-60aa020%20authorised.pdf](http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/6BF03254A893AFC4CA258314001B4CF2/$FILE/14-60aa020%20authorised.pdf)

Health Records Act 2001 (Vic)

[http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/274F3FF5B9152CF9CA258314001B0814/\\$FILE/01-2aa040%20authorised.pdf](http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/274F3FF5B9152CF9CA258314001B0814/$FILE/01-2aa040%20authorised.pdf)

Charter of Human Rights and Responsibilities Act 2006 (Vic)

[http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt8.nsf/DDE300B846EED9C7CA257616000A3571/87318807B8E7A33ACA257D0700052646/\\$FILE/06-43aa013%20authorised.pdf](http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt8.nsf/DDE300B846EED9C7CA257616000A3571/87318807B8E7A33ACA257D0700052646/$FILE/06-43aa013%20authorised.pdf)

Surveillance Devices Act 1999 (Vic)

[http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/94BE26A181B7C22ACA2582FD000859EA/\\$FILE/99-21aa037%20authorised.pdf](http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/94BE26A181B7C22ACA2582FD000859EA/$FILE/99-21aa037%20authorised.pdf)

Child Wellbeing and Safety Act 2005 (Vic)

[http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/191E231BE2CDE48BCA25833800048603/\\$FILE/05-83aa025%20authorised.pdf](http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/191E231BE2CDE48BCA25833800048603/$FILE/05-83aa025%20authorised.pdf)

Authorised by Industrial Relations Victoria:

Key Details	Date
Version	Final as approved
Date	December 2021

If you print and store this document, you may be looking at an obsolete version. Always check the latest version of this document on the intranet.