# Court Services Victoria

# Acceptable Information and Communications Technology Usage Policy

## Purpose

This policy provides guidance on acceptable usage of Court Services Victoria (CSV) information and communications technology (ICT) resources.

## Scope

This policy applies to all CSV employees, volunteers, contractors, consultants and any other individual or group using CSV's ICT resources.

The policy applies to all workplaces, work activities of CSV and ICT resources.

## Legislative and Policy Context

This policy should be read in conjunction with the:

- Code of Conduct for Victorian Public Sector Employees 2015 (Code of Conduct),
- *Privacy and Data Protection Act 2014* (Vic),
- *Public Records Act 1973,* and
- *Freedom of Information Act 1982.*

## Principles

This policy has been developed in accordance with the following principles:

- ICT is a critical tool for the efficiency of CSV business.
- Maintaining the reputation of CSV and sustaining public trust and confidence.
- CSV provides access to ICT resources to enable CSV employees to deliver agreed CSV work activities
- ICT resources are used appropriately and professionally at all times, having regard to reasonable working hours and meeting the needs of employees to balance their work and personal responsibilities.

## Policy

CSV aims to create an environment of exemplary work standards and conduct, and to ensure high levels of positive public opinion.

Employees, volunteers, contractors, consultants and other third parties that have access to CSV systems and information are expected to adhere to the Code of Conduct. This policy provides further guidance regarding the expected standards for the acceptable use of CSV's ICT resources.


CD/16/358920

## Responsibilities

| Group | Responsibility |
|---|---|
| **Employees, volunteers, contractors, consultants, individuals or groups using CSV ICT resources** | • perform duties with honesty, integrity, professionalism and respect as set out by the Code of Conduct,<br>• only use CSV ICT resources as authorised, in a legal, ethical manner, complying with relevant legislation, applicable policies, procedures and guidelines,<br>• report any concerns or potential security incidents to management and/or CSV's ITS Security team or relevant court/tribunal technology team. |
| **Managers** | In addition to the above and without in any way limiting the other provisions of this policy, all managers (and supervisors) must:<br>• ensure all staff are aware of their responsibilities and adhere to the contents of the Acceptable ICT Usage Policy,<br>• ensure any matters raised under this policy are managed in accordance with its terms,<br>• notify CSV's Information Technology Services (ITS) Security team or relevant court/tribunal technology teams of any potential information security incident,<br>• take appropriate action to prevent the misuse of CSV's ICT resources, and<br>• take immediate action to stop conduct in breach of this policy if they consider it is occurring. |

## Acceptable use

Users of CSV ICT resources:

- must use such resources primarily for CSV business (refer to Personal use of CSV ICT resources section below),
- must protect and look after the physical condition of ICT assets and not deliberately damage such resources,
- must protect the state of software on the computer by not connecting unauthorised devices or networks and making use of security software,
- should maintain the integrity, accuracy and confidentiality of information accessed, through appropriate classification and handling of information, and secure use of portable storage devices,
- must keep passwords confidential,
- may only use CSV systems and approved third party services to store, process or transmit CSV information, in order to ensure protective measures are in place,
- should always communicate in an appropriate and professional manner, and avoid using language or saving/copying and distributing content that may cause offence,
- may only open or share another person's email from their email account when delegated by the account owner to do so and it is part of duties to meet business requirements or formally authorised by CSV CIO or relevant Jurisdiction CEO,
- should show caution when opening unsolicited email and clinking on links or opening attachments within such communications, and notify appropriate ITS personnel of any suspicious emails.
- should be aware that whilst access to CSV ICT resources may facilitate flexible working arrangements, CSV is committed to workplace health, safety and wellbeing for employees, including ensuring that employees are not routinely required to perform excessive work hours.

**Personal use of CSV ICT resources**
Incidental personal use of CSV is permitted, providing it is:

- reasonable (i.e. not excessive),
- appropriate,
- not affecting the performance of CSV duties,
- not related to a private business (e.g. unrelated to your employment by CSV), and
- not breaching any relevant legislation (e.g. copyright, intellectual property, privacy).

It is also relevant to note that use of personal and other non-CSV systems (e.g. personal email accounts) for CSV business is prohibited unless approved by a manager, with agreed protective measures suitable to the sensitivity of the information.

## Unacceptable use

Unacceptable use of CSV's ICT resources includes, but is not limited to:

- use for any personal profit,
- use for purposes not directly related to the business of CSV (incidental/personal use is permitted, refer to 'Personal use of CSV ICT resources' section above),
- use to copy, retrieve, or forward confidential or sensitive information (e.g. database files including information held on court management systems such as Courtlink, Courtview or CLMS, documentation, articles, graphics files and downloaded information as defined by CSV and the court, tribunal, Judicial College of Victoria (JCV) or Judicial Commission of Victoria (the Commission)) unless it is authorised by the corresponding information owner,
- use to copy, retrieve, or forward confidential or sensitive information to non-CSV or court/tribunal/JCV/Commission authorised portable or mobile devices (e.g. notebooks, USB drives, iPads or mobile phones) unless it is authorised by the corresponding information owner,
- use to copy, retrieve, or forward confidential or sensitive information to non-CSV or court/tribunal/JCV/Commission authorised ICT / cloud services (e.g. Dropbox, Google drive or external web mails) unless it is authorised by the corresponding information owner,
- use to copy, retrieve, or forward confidential or sensitive information to personal emails systems (e.g. Gmail, Hotmail, Yahoo, etc.) unless it is authorised by the corresponding information owner,
- use of unauthorised instant messaging clients, including web-based clients (e.g. Yahoo Messenger; MSN Messenger; Google Talk; Whats App; WeChat, Viber) for official CSV business,
- sending any chain mail or advertising material,
- use of CSV's email business addresses for private purposes or registering on public websites (e.g. Facebook, forums, etc.) unless there is a business need and by agreement with the employee's manager (refer to Social Media Policy for more information),
- development or use of programs designed to harass other users or infiltrate a computer or computer network or to damage or alter hardware or software,
- installation of unauthorised software without prior approval from ITS, Jurisdiction Services (JS) or in circumstances where a court/tribunal provides its own network, then the court/tribunal's ICT Manager,
- search for, download, display, transmit or store any material which may be considered fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate,

- use for inappropriate activities for example, pornography, fraud, defamation, breach of copyright or the intellectual property rights of others, unlawful discrimination or vilification, harassment (including sexual harassment), racism, stalking, bullying, hacking, privacy violations, perpetrating family violence and illegal activity, including illegal peer-to-peer file sharing, and/or
- use of services to conceal your identity while using CSV ICT resources.

Employees, contractors, consultants and other users of CSV ICT resources should speak to their manager or supervisor if they are unsure about what is acceptable use of CSV's ICT resources.

### Access and monitoring

All electronic communications created, sent or received using CSV's ICT resources email systems are the property of CSV. All information produced on CSV's ICT resources, may be accessible under the *Freedom of Information Act 1982 (Vic)*.

Employees should be aware that CSV's ITS Security team, with agreement from and authorisation of courts and tribunals, JCV, the Commission, and/or JS, will, at times, access or monitor the use of its ICT systems, including content of electronic communications.

The contents of ICT systems may be reviewed:

- where it is required by law,
- to ascertain compliance with CSV's policies and procedures ,
- where required for the purposes of an investigation,
- to protect the security of CSV ICT facilities and services, and/or
- to satisfy the requirements of the *Freedom of Information Act 1982 (Vic).*

Monitoring of system access and use is generally conducted at the court/tribunal/business area level. Indicators requiring further investigation with a view to identifying inappropriate or excessive personal use by an individual is managed in accordance with CSV's Misconduct Policy.

## Definitions

| | |
|---|---|
| **Court Services Victoria** | includes courts, tribunals, Judicial College of Victoria, Judicial Commission of Victoria and Jurisdiction Services. |
| **Email** | refers to all forms of electronic mail and messaging, other than instant electronic messaging. |
| **ICT resources** | resources which store, retrieve, manipulate, transmit or receive information electronically in a digital form, including networks, systems, software and hardware (for example, wireless networks, local area networks, wide area networks, software, servers, computers, email, internet, intranet, mobile phones, tablets/iPad, printers, portable storage devices, cloud services, etc.). |
| **Internet** | A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols. |
| **Intranet** | is a facility that enables information sharing using an organisation's internal communication network and has similar features to the internet. |

## Related policies and other documents

CSV's Information Technology Services policies and standards
Information Privacy Policy
Misconduct Policy
Respect in the Workplace Policy
Social Media Policy

## Version control

| Version | Approved by | Date of Approval | TRIM Reference |
|---|---|---|---|
| 0.1 | HR Portfolio Committee | 22 May 2017 | CD/16/358920 |
| 0.2 | HR Policies Working Group | 19 February 2018 | CD/16/358920 |
| 1.0 | Chief Executive Officer, CSV | 26 March 2018 | CD/16/358920 |