



Acceptable Use of Resources Policy

Purpose

The purpose of this Policy is to outline how Victorian School of Commerce (VSC) resources should be used and to define what VSC considers acceptable and unacceptable uses of its resources. It outlines the expectations and obligations of VSC visitors, students, staff, contractors, and consultants when using resources provided by VSC. It also addresses the implications for breaches of this policy.

Scope

This Policy applies to all students, academic and non-academic staff, Board and Committee members and contractors of VSC. It is the responsibility of each of these individuals to comply with this policy as a condition of access to VSC Resources.

Definitions

Hardware means all physical equipment provided by VSC for staff or student use. This includes computers, monitors, photocopiers, printers, telephones or any other physical resource provided by VSC for staff or student use.

Resources means any resource, or access to any resource, provided by VSC to Users. This includes, but is not limited to, Hardware, Software, internet access, email access or any other resource whether physical or virtual provided by VSC. Resources may include, but is not limited to, the following:

- Desktop computers
- Monitors or displays
- Laptops
- Tablets
- Computer accessories (wireless keyboard/mouse, speakers etc)
- Mobile phones
- Desktop telephones
- Photocopiers
- Printers
- Physical library resources
- Virtual library resources
- Internet access
- Data storage, both physical and virtual
- Email access
- Software



- Furniture

User means all permanent staff, casual staff, sessional staff, contractors and students at VSC.

Policy

1.1. Provision of Resources

VSC provides Resources to Users in the course of delivering educational services, training, assessment, teaching and learning, research endeavors and administrative services. VSC provides resources to support VSC visitors, students, staff, contractors and consultants as part of their work and/or experience with VSC. The integrity and security of VSC Resources are critical to VSC operational safety and business reputation. For that reason, VSC Resources are managed appropriately and users are expected to use VSC Resources in accordance with the standards set out in this Policy.

1.2. Authorised Use of Resources

VSC expects that Users only utilise Resources for authorised purposes. The access to VSC Resources will be determined and authorised by the direct supervisor of the staff and by the lecturer for the students. Authorised use includes, but is not limited to, the following:

- 1.2.1. Staff use relevant to their employment with VSC
- 1.2.2. Student use relevant to their enrolment with VSC
- 1.2.3. Contractor use relevant to their engagement with VSC

Users are responsible for their own usage and are allowed to access only those Resources for which they have been authorised. In order to ensure integrity and security, the Users should never allow any other person to use VSC Resources, password or login details for accessing VSC system. Users are expected to:

- Utilise VSC provided resources in an appropriate and safe manner that does not damage or impair the resources; and
- Consider their safety and the safety of others when utilising VSC provided resources and must not utilise resources if there is a safety concern.

1.3. Personal Use

VSC allows limited and reasonable personal use of Resources. This is on the basis that the personal use does not interfere with the User's role within VSC, the work or study of others or the operation of the systems. Personal use does not include any use of Resources for conducting a personal business or private commercial activity, gambling or carrying out excessive and regular research into topics not related to the User's employment, engagement or enrolment at VSC.

1.4. Intellectual Property Rights

Unless otherwise specifically stated elsewhere in written agreements, VSC will have ownership of all intellectual property created by staff and contractors as part of their



employment or engagement with VSC. VSC will also have ownership of all data created, sent or received by all Users utilising VSC's Resources.

1.5. Privacy

All Users must utilise Resources to ensure compliance with VSC's *Privacy Policy*. As such, all use of VSC resources may be monitored and recorded and may take appropriate actions in case any misuse of these resources is identified.

1.6. Social Media

Users must respect the purpose of and abide by the terms and conditions of use of online forums, including social media networking websites, mailing lists, chat rooms, wikis and blogs. Users must demonstrate respect towards others. Defaming, vilifying, bullying or harassing someone in the social media may result in disciplinary actions.

1.7. Unauthorised Use of Resources

While VSC recognises that personal use of resources may be required occasionally, VSC does not allow the unauthorised use of its Resources. Any User who utilises VSC Resources in an unauthorised manner may face disciplinary action.

Examples of unauthorised use of VSC Resources include, but is not limited to, the following:

- 1.7.1. Sending, viewing, downloading or storing illicit, fraudulent, obscene or pornographic material that are a violation of applicable law or VSC Policy or Procedure.
- 1.7.2. Using Resources for the purpose of conducting an outside business.
- 1.7.3. Using Resources for commercial uses such as advertising or selling.
- 1.7.4. Using Resources for any illegal activity.
- 1.7.5. Using Resources in violation of any VSC Policy or Procedure;
- 1.7.6. Using Resources to defame, harass, bully, abuse or act in any manner which may breach any law or VSC's *Code of Conduct, Bullying, Discrimination and Harassment Prevention Policy, Equity and Diversity Policy* or any other Policy or Procedure.
- 1.7.7. Using Resources to engage in any actions resulting in Domestic and Family Violence.
- 1.7.8. Using Resources to violate copyright law or anyone else's intellectual property rights.

All Users of resources at VSC are expected to use them in a reliable and safe manner, as well as to use them in such a way that no damage or impairment is done to the Resources. Users need to not only consider their own safety when utilising resources, but also the safety of others.

Software Licenses



Software purchased by VSC is licensed primarily to VSC, however, approval may be granted to authorised users for use at home or other locations of non-VSC owned computers during the course of work or study with VSC in accordance with the *Acceptable Use of Resources Policy*.

Authorised users must comply with contractual obligations and terms of conditions of use stated in the software license agreements entered into by VSC.

Authorised Users must discontinue use and un-install the software from non-VSC owned computer(s) upon cessation or termination of employment or completion of study, or upon notification by VSC of its termination of the software license agreement.

Monitoring and Privacy

VSC reserves the right to monitor, access, log and analyse the activities of Authorised Users, and of VSC ICT Services, and conduct reviews and audits as necessary.

VSC reserves the right to block or filter any use that breaches this Policy or exceeds VSC's acceptable level of risk.

Subject to the provisions of VSC's *Privacy Policy* and relevant legislation, VSC may disclose the contents of electronic communications without permission of the Authorised User.

VSC may take any action deemed necessary to remedy immediate threats to VSC ICT Services or information and communications technology security including, without limitation, suspending an Authorised User's access, confiscation of VSC owned electronic devices and/or disconnecting or disabling equipment with or without prior notice.

Consequences of breach

Breaches of this Policy may be grounds for misconduct/serious misconduct.

A breach or alleged breach of this Policy may result in a referral of the matter to the police and/or other relevant external law enforcement authority for investigation.

VSC reserves the right to immediately suspend or restrict access to an Authorised User's account in the case of a breach or an alleged breach of this Policy.

If an alleged breach of this Policy is reported, action will be taken in accordance with the *Acceptable Use of Resources Policy* including action taken to protect a person who has made a Public Interest Disclosure or action taken in respect of suspected Corrupt Conduct.

Related policy instruments

Bullying, Discrimination and Harassment Prevention Policy

Code of Conduct

Conflict of Interest Policy

Critical Incident Management and Business Continuity Policy



Equity and Diversity Policy

Facilities, Resources and Infrastructure Policy

Health and Safety Policy (Staff & Students)

Library Policy

Privacy Policy

Records and Information Management Policy

Risk Management Policy

Student Handbook (Domestic)

Student Handbook (International)

Student Wellbeing and Support Policy

Student Wellbeing and Support Procedure

Student Complaints and Appeals Policy and Procedure

Student Complaints and Appeals Procedure

Staff Complaints and Appeals Policy and Procedure

Staff Complaints and Appeals Procedure

Related documents and legislation

Freedom of Information Act

Independent Broad-based Anti-Corruption Commission Act 1022 (Vic)

Privacy and Data Protection Act

Administration

Revision History

Version	Approval date	Approval body	Review date
0.1	20/01/2020	Board of Directors	
0.2	18/02/2020	Board of Directors	
1.0	18/06/2021	Board of Directors	30/06/2022