VECTOR INSTITUTE | INSTITUT VECTEUR

Appropriate Use of Information Communications Technology Policy

1. Purpose

Vector provides its technology systems, services, and data ("Technology Assets") to support its research, educational, and administrative mandates. Vector's Technology Assets must be used in a manner consistent with its status as a not-for-profit corporation, with all related and supporting technology and data governance policies, in accordance with its Code of Conduct, and in compliance with all applicable federal and provincial laws.

The Appropriate Use of Information Communications Technology Policy outlines requirements and responsibilities of any individual being given access to Vector's Technology Assets in order to safeguard these assets from accidental or intentional misuse.

2. Scope

This Appropriate Use of ICT Policy (the "Policy") applies to anyone who is granted permanent or temporary access to Vector's Technology Assets.

As a user of Vector's Technology Assets, you may have access to valuable internal and external technology systems, services, and data including sensitive information, which you are expected to use in a responsible, ethical, and legal manner.

Your actions should not adversely affect the ability of others to use these assets, nor compromise the security and privacy of sensitive information.

This Policy covers all of Vector's Technology Assets, as well as the services that are provided through them, including, without limitation, email, internet access, wireless network services, telephone, voicemail, and other technologies, including social networking channels.

The Policy also applies to personal devices connected to Vector's network such as a personal laptop, mobile device, or WiFi-enabled device.

3. Policy Principles

Users are responsible for familiarizing themselves with, and abiding by, policies and regulations regarding the appropriate use of technology assets, including Vector's Code of Conduct, Workplace Harassment, and other related policies found on the Policy page of the Vector website.

Ignorance of Vector policies does not negate the requirement to comply with said policies.

Vector is committed to maintaining respect for the core value of academic freedom.

While Vector does not censor information on its networks and servers, it will act on allegations regarding the distribution of unlawful material, the use of its Technology Assets to direct abusive, threatening, or harassing communication at any individual or group of individuals, or any other inappropriate use of its Technology Assets.

Access to Vector's Technology Assets is a privilege, accompanied by a corresponding obligation to behave responsibly.

This includes, but is not limited to, the following:

A. ***Privacy:*** Vector respects the privacy of electronic files stored or distributed on its servers and networks; however, unless expressly provided otherwise, these files remain the property of Vector and can be accessed

and inspected at any time at the direction of the CEO, COFO, CDO, or CIO. Individuals using Vector's Technology Assets recognize that they have a limited expectation of privacy therein.

Vector has the right, but not the obligation, to audit and inspect usage of its Technology Assets at its discretion for the purposes of oversight for audit and inspection, compliance with terms of use, enforcement of government accountability agreements, and other agreements that Vector may enter into, and compliance with laws and regulations.

Unauthorized access to any Technology Asset user of another individual's electronic information is a violation of this Policy.

B. ***Inappropriate use of Technology Assets:*** Every user of Vector's Technology Assets must use the Assets in an appropriate manner. Inappropriate use includes, but is not limited to, the following:

   a. Use of Technology Assets for non-Vector related activities, outside of incidental personal use. Incidental personal use may not interfere with Vector's activities, and personal use may not result in additional cost to Vector.

   b. Use of Technology Assets to operate or advertise a business or other commercial enterprise that has not been authorized in advance by authorized Vector personnel.

   c. Use of Technology Assets to access, create, publish, process, download, or communicate material, information or content that is illegal (including in violation of the Ontario *Human Rights Code*, copyright, intellectual property or other laws, guidelines or agreements), infringing, privacy invasive, pornographic, obscene, abusive, derogatory, defamatory, offensive, harmful, tortuous, hateful, racially, ethnically or otherwise objectionable, discriminatory, harassing, threatening, or violent in nature. Any activity contravening Vector's Code of Conduct goes against this Policy.

   d. Attempting to, or actually, violating or infringing any other person's intellectual property and related rights (including copyright).

   e. Intentional interference with the normal operation of Technology Assets including, but not limited to, spreading malware, rootkits, viruses, using unsecure IT hardware such as data storage devices, flooding the network with messages, sending chain letters or solicitations, excessive streaming or other use of bandwidth, attempting to disable or compromise the security of information, etc.

   f. Vandalising or attempting to vandalise or damage any Technology Asset.

   g. Using, publishing, downloading, communicating, uploading or distributing any unlicensed or illegal digital content (including data, code, software, media, etc.) in any manner using Vector Technology Assets.

   h. Use of Assets to transmit or post any material or content that encourages conduct that constitutes either a criminal offense or gives rise to civil liability.

   i. Use of Vector Technology Assets to promote specific political opinions, persons, parties, or interests.

   j. Using, publishing, downloading, communicating, uploading or distributing on any Technology Assets any content, material or information that violates any applicable laws or in a manner that may violate any applicable laws.

   k. Providing access to Vector Technology Assets to anyone else (e.g., students, staff, or guests), unless explicitly authorized, in advance and in writing, by Vector.

l. Accessing any other person's professional or personal social media accounts, email, data or personal information using Vector Technology Assets without prior express prior written permission from that person.

m. Use of prohibited technology as identified in Schedule A: Prohibited Technologies List.

C. ***Confidentiality and Unauthorized Disclosure of Information:*** You will not, at any time during your affiliation with Vector or afterwards, disclose to any person any confidential information about Vector, its partners, or its industry sponsors.

There may be some exceptions when working on projects with industry sponsors; please consult with your immediate supervisor before engaging in any projects. Any disclosures of confidential information (including personal information kept on laptops or devices) outside the proper course of duty will be treated as a breach of this Policy and any applicable contract.

D. ***Account Integrity:*** All Users are responsible for maintaining the integrity of their own Technology Assets, taking reasonable measures to secure their accounts and/or hardware with strong passwords and/or access codes, ensuring software is regularly updated, and any other measures suggested by Vector's Technology teams, including physical safety and security measures.

Users must implement appropriate safeguards to secure Technology Assets against theft, damage or unauthorized access. Users shall always ensure that they safeguard confidential information using reasonable measures, at least as stringent as those typically used by the receiving party, to protect personal information.

Users must also comply with all applicable private and data protection legislation and with related privacy policies as then in effect (e.g., the privacy policies of an affiliated academic institution). Users may not disclose passwords or account information to any other person.

E. ***Email/Social Communication Channels:*** Email use should comply with Vector's applicable policies without compromising current Technology Assets and safety standards. This includes refraining from activities such as sending spam, "junk mail", chain letters, or unsolicited mass distribution of email, or opening harmful or malicious links sent by unknown users.

Individuals must be mindful and must not share any information about: industry sponsors, human resources and personnel-related matters, intellectual property, trade secrets, and any other sensitive information.

Communications channels include, but are not limited to, Slack, web interfaces, Google Groups, and other social media.

F. ***Internet Activity:*** Any internet usage should adhere to Vector's policies and practices as well as align with the goal of supporting the administrative, educational, instructional, and research functions of Vector.

Internet access must not be used to visit illegal websites or to download unrelated, inappropriate files that may contravene the Workplace Harassment or Workplace Violence policies, or any provision of the Ontario *Human Rights Code*.

Vector's Technology team may audit and inspect a user's internet activity at Vector's discretion, with confidential reports provided to Vector's senior leadership for the purposes of oversight, compliance, and security.

G. ***Vector Marks:*** Vector and Vector's licensors own all rights, title, and interest (including intellectual property rights) throughout the world in, to, and associated with Vector Marks.

Vector Marks include the trademarks, service marks, logos, and other trade indicia owned by or licensed to Vector. Guests and users do not have and will not acquire any license or right to use any Vector Mark except as expressly permitted under this Policy or as otherwise permitted in writing by Vector.

Under no circumstances can Vector Marks be used in marketing, advertising, publicity, solicitations, news releases, or promotions that have been disapproved or have not been expressly approved by Vector. The use of Vector Marks in either citation or publication does not provide ownership, rights, or title to such Vector Marks.

H. ***Geo-Blocking:*** To ensure the integrity and security of organizational resources, Vector enforces geo-blocking as one of its cybersecurity controls. Geo-blocking restricts access to and from countries identified as national cybersecurity threats. This measure is designed to safeguard sensitive data and systems from potential external risks originating from these regions. Anyone who is granted permanent or temporary access to Vector Technology Assets is expected to comply with this restriction and must not attempt to bypass or circumvent geo-blocking controls under any circumstances.

I. ***Network Access Control:*** To ensure the integrity and security of its network, Vector employs a Network Access Control (NAC) system to enforce minimum security standards for devices connecting to the corporate network. Only devices that meet minimum security standards will be granted network access to ensure the security of Vector's network and compliance with internal policies. Anyone connecting to Vector's network is responsible for ensuring that their devices meet these standards before attempting to connect to the network.

4. Consequences for Non-Compliance

Vector considers any violation of this Policy to be a serious offense and reserves the right to restrict access to any and/or all Technology Assets in case of a breach. Access may be returned at Vector's sole discretion.

In the event of a violation, Vector will exercise its rights to take appropriate disciplinary action in its sole discretion. This may include, but may not be limited to:

- verbal or written warnings;
- rescinding, suspending, and/or restricting access to Technology Assets;
- removal of materials from Vector computer equipment, facilities, and networks;
- removal of Vector computer equipment, facilities, and networks;
- disciplinary action such as suspensions;
- termination of employment or affiliation; and
- prosecution of charges and reporting a breach to the appropriate regulatory and law enforcement agencies, as well as any affiliated institutions (e.g., hospitals and universities). Such agencies and institutions may, in turn, take their own enforcement actions for cross-appointed personnel such as faculty and researchers.

5. Amendment

Vector may amend this Policy, and future amendments will be made as Vector's Technology Assets grow.

Members of the Vector community will be advised of any future amendments and will be expected to become familiar with and abide by the then-current version of this Policy.

Schedule A: Prohibited Technologies List

In order to maintain the security, integrity, and efficiency of Vector's operations, specific software, equipment, and services are prohibited within the organization. These technologies have been deemed inappropriate or unnecessary for business needs, and/or they pose unacceptable security risks to Vector's Technology Assets.

The prohibited technologies include items that may compromise sensitive information, introduce vulnerabilities, or conflict with Vector's operational policies and objectives. These restrictions apply to all employees, contractors, and third-party partners when using the organization's equipment, accessing its services, or connecting to its networks.

Prohibited Technology	Category	Notes
Peer-to-peer (P2P) file sharing services	Service	Peer-to-peer (P2P) file sharing services such as BitTorrent are prohibited because they are not required to support Vector business and their use is often linked to the illegal transfer of copyrighted and/or inappropriate content. P2P sites also pose security risks, as these sites are targeted by threat actors by using false file descriptions to spread malware and ransomware.
TikTok	Mobile App	TikTok's collection of personal information, browsing history, and location data raise concerns about the potential for misuse (e.g., controlling user feeds, suppressing dissent, or spreading disinformation) by foreign actors deemed a cybersecurity threat to Canada.
DeepSeek App	Mobile App	Research on the DeepSeek App has identified a range of security concerns including unencrypted data transmission, hardcoded encryption keys, insecure storage of credentials, fingerprinting, and disabled iOS Privacy Controls.