

## Appropriate Use of Information and Communication Technology Policy

### Policy Statement

This Appropriate Use of Information and Communication Technology (ICT) Policy (the “Policy”) applies to all members of the community at the Vector Institute (“Vector”), including employees (permanent or contract), students, alumni, guests, and other individuals who, within their role and responsibilities have been granted access or permission to access certain data, information, applications or systems that are part of Vector’s technology resources.

As a member of the Vector community, you may have access to valuable internal and external networks and resources, 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 resources or compromise the security and privacy of sensitive information.

### 1. Purpose and Scope

Vector owns and manages information and communication technology resources (“ICT Resources”) to support the educational, instructional, research and administrative functions of Vector. The use of Vector’s ICT Resources must be consistent with Vector’s values of integrity, honesty and accountability and must be in compliance with Vector’s other applicable policies.

An ICT Resource includes any computing/peripheral/media device that may or may not have the ability to connect (wired, wirelessly, or cellular) to Vector’s network including, but not limited to, cloud computing services, hardware (e.g., personal computers, cellphones, portable devices, printers/scanners, cabling, etc.), software, databases or records systems, and any copies or backups of any of the foregoing. ICT Resources also include Vector’s network itself.

This Policy covers all of Vector’s ICT Resources as well as the services that are provided through them, including without limitation e-mail, internet access, wireless network services, telephone, voicemail, and other technologies including social networking channels.

### 2. Policy Principles

Users are responsible for familiarizing themselves with and abiding by policies and regulations regarding the appropriate use of technology resources including Vector’s Code of Conduct, Harassment, and other related policies. Ignorance of Vector policies does not negate the requirement to comply with said policies.

Vector is committed to maintaining respect for the core values of freedom of speech, academic freedom, and freedom of research. 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 ICT Resources to direct abusive, threatening or harassing communication at any individual or group of individuals, or any other inappropriate use of its ICT Resources. Access to Vector’s ICT Resources 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 President and CEO or COO/CFO. Individuals using Vector’s ICT Resources recognize that they have a limited expectation of privacy therein. Vector has the right, but not the obligation, to audit and inspect usage of computing systems (e.g., encrypted devices will be

accessible through sharing of the decryption key) at the discretion of Vector, with confidential reports provided to Vector's senior leadership for the purposes of oversight for audit and inspection, compliance with terms of use, and enforcement of government accountability agreements, and other agreements that Vector may enter into e.g., checking and enforcing the terms of sponsored research agreements or oversight and enforcement of corporate policies. Unauthorized access by any Vector community member of another individual's electronic information is a violation of this Policy.

- b. **Inappropriate use of information and communication technology:** Every user of Vector's ICT Resources must use ICT Resources in an appropriate manner. Inappropriate use includes, but is not limited to, the following:
- Use of ICT Resources for personal or for non-Vector related activities.
  - Use of ICT Resources to operate or advertise a business or other commercial enterprise that has not been authorized in advance by authorized Vector personnel.
  - Use of ICT Resources 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.
  - Attempting to, or actually violating or infringing, any other person's intellectual property and related rights (including copyright).
  - Intentional interference with the normal operation of ICT Resources 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.
  - Vandalising or attempting to vandalise or damage any ICT Resources.
  - Using, publishing, downloading, communicating, uploading or distributing on any ICT Resources and in any manner, any software, code, files, or other material, content or information that may contain or contain any viruses, corrupted files, worms, or other computer code that has or may have the effect of disabling or interrupting the operation of a computer system, or destroying, erasing or otherwise harming or compromising any data, software, or hardware.
  - Use of ICT Resources to transmit or post any material or content that encourages conduct that constitutes a criminal offense or gives rise to civil liability.
  - Using, publishing, downloading, communicating, uploading or distributing on any ICT Resources any content, material or information that violates any applicable laws or in a manner that may violate any applicable laws.
  - Extending the access level or privilege of ICT Resources to anyone else (students, staff, or guests), unless explicitly authorized, in advance and in writing, by Vector.
  - Accessing any other person's social media accounts, email, data or personal information without prior express prior written permission from that person.
- 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 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 staff are responsible for maintaining the integrity of their own IT account and ICT Resources, 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 scientific computing team or Systems Operations Manager, including physical safety and security measures. Users must implement appropriate safeguards to secure technology resources 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 (i.e. Confidentiality Policy, Code of Conduct & Harassment Policy, etc.) without compromising current IT infrastructure 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, HR 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 educational, instructional, research and administrative 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 scientific computing team and Systems Operations Manager 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 which have been disapproved or not approved by Vector. The use of Vector Marks in either citation or publication does not provide ownership, rights, or title to such Vector Marks.

### 3. 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 ICT Resources 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 ICT Resources;
- 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 charges and reporting breaches to the appropriate regulatory and law enforcement agencies, as well as any affiliated institutions e.g. hospitals and universities.

#### **4. Amendment**

Vector may amend this Appropriate Use of Information and Communication Technology Policy, and future amendments will be made as Vector's IT infrastructure grows. 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.