 <p>Capilano Students' Union</p>	<b>Policy No.</b>	<b>Approval Authority</b>
	HR-09	Board of Directors
	<b>Policy Name</b>	<b>Approval Date</b>
	<b>Acceptable Use</b>	May 31, 2024
	<b>Responsible</b>	<b>Scheduled Review</b>
	Executive Director	2 years

## Purpose


The purpose of this policy is to set out expectations for the acceptable use of Capilano Students' Union technology by internal users, in order to protect the security and integrity of the organization's information systems.

## Scope

This policy applies to all managers, employees, student executives, board members, committee members, volunteers, contractors, and anyone else who accesses any Capilano Students' Union devices (such as tablets, laptops, or desktop computers) or accounts (such as Capilano Students' Union email accounts).

## Principles

- 1. Standard of Conduct.** All users are expected to use Capilano Students' Union devices and accounts in accordance with the [standard of conduct policy \(HR-08\)](#) or the [board ethics and conduct policy \(BD-01\)](#), as applicable.
- 2. Protected Information.** Capilano Students' Union devices and accounts may include access to information that is protected under the [information classification policy \(PR-02\)](#). All users are responsible for preventing unauthorized access to protected information. If a device is lost or stolen, or an account is compromised, this must be reported to the executive director right away so that steps can be taken to lock down that device's access.
- 3. Logical Access.** Users must be provided with the lowest level of access to protected information that they require to do their job. We promptly revoke account access for users who leave the organization, and access levels are reviewed regularly to ensure that they are still providing appropriate levels of access.
- 4. Account Security.** Managers, employees, student executives, and board members are expected to maintain the security of user accounts that have been assigned to them. Usernames and passwords should never be shared.

 <p>Capilano Students' Union</p>	<b>Policy No.</b>	<b>Approval Authority</b>
	HR-09	Board of Directors
	<b>Policy Name</b>	<b>Approval Date</b>
	<b>Acceptable Use</b>	May 31, 2024
	<b>Responsible</b>	<b>Scheduled Review</b>
	Executive Director	2 years

**5. Software.** Given the widely varied privacy policies of developers, and the need to ensure that protected information on Capilano Students' Union devices and accounts is secure, only approved software or apps can be installed on Capilano Students' Union devices or connected to Capilano Students' Union accounts. New software or apps can be approved by staff designated by the executive director after giving appropriate consideration to the app's security reputation, requested access permissions, and privacy policy.

**6. Accountability.** Everyone who uses Capilano Students' Union devices or accounts is responsible for using those devices or accounts appropriately, per this policy, and there are consequences for non-compliance.

### Delegation

The board delegates the administration of this policy, and the authority to create technology procedures and programs to support this policy, to the executive director.

### Review and Monitoring

The finance and audit committee monitors compliance with this policy and is responsible for reviewing this policy every two years and recommending necessary updates to the board.

### Related Laws, Policies, and Procedures

- [Policy PR-01: Privacy](#) (Capilano Students' Union)
- [Policy HR-08: Employee Standard of Conduct](#) (Capilano Students' Union)
- [Policy BD-01: Board Ethics & Conduct](#) (Capilano Students' Union)