Capilano Students' Union	Procedure Name	Approval Authority
	Privacy Procedures	Executive Director
	Created Under	**Approval Date**
	Privacy Policy	**August 18, 2017**
	Responsible	**Scheduled Review**
	Executive Director	August 2018

Processing Requests

Requesting Access and Corrections

Requests to access personal information should be made as follows:

1. The applicant should contact the Capilano Students' Union at privacy@csu.bc.ca to request access to personal information; the applicant should be asked to provide as much specific detail as possible about the personal information being requested.

2. The privacy officer shall review the request and either:
    a. Assign an employee to facilitate access to the requested information in a manner that satisfies the applicant's request, such as through photocopies of records, an in-person inspection of records by the applicant, or through some other means; or
    b. Decline the request for access, and provide written reasons.
3. An access request must be resolved within thirty (30) business days.
4. If an applicant becomes aware that there is inaccurate or out-of-date personal information belonging to them that is held by the Capilano Students' Union, the applicant may request that corrections be made to the personal information. The privacy officer is responsible for providing direction to employees to ensure that the corrections are made.

Complaints

In the event that a person disagrees with a decision made by the Capilano Students' Union with respect to a request to access or correct personal information, or any other privacy-related matter, a complaint should be made as follows:

1. The complainant should contact the Capilano Students' Union at privacy@csu.bc.ca and provide the written particulars of the complaint in as much detail as is possible.
2. The privacy officer shall review the complaint and reply within thirty (30) business days. If the complaint is valid, then the privacy officer shall provide direction to staff to ensure that any inadequate privacy practices or controls are remedied without delay.
3. If a complainant disagrees with a decision made by the privacy officer under this procedure, then the privacy officer shall provide the complainant with contact information for the Office of the Information and Privacy Commissioner of British Columbia, and explain how to appeal.

Personal Information Security

Login Credentials

Usernames and passwords should never be shared between users. Individual user accounts should be used wherever possible – this also ensures that the organization can review access and sharing changes that are made by users when it comes to confidential or personal information. Users shall be required to change passwords at irregular intervals, and at least twice per year.

Secure Transmission by Fax

In the event that personal information needs to be sent by fax:

1. The sender should contact the recipient to ensure that the receiving machine is attended.

2. Use a verified, pre-programmed fax number where possible.
3. If you must dial manually, visually double-check the recipient number before sending.
4. Use a standard fax cover sheet, including the number of pages being transmitted.
5. Check the fax confirmation as soon as it has been generated.

If you believe that a fax containing personal information has been sent to an incorrect recipient, contact the unintended recipient right away and request that the document be destroyed, and then contact the executive director. Extremely sensitive personal information (such as a social insurance number or medical history) should never be sent by fax, even if the above precautions are used.

Review of Audit Logs

Once per month, the executive director shall review the audit logs and permission levels for all users of the csu.bc.ca domain and G Suite services for unusual or unauthorized activities. Any substantial unauthorized activities shall be brought to the attention of the executive committee for approval.

Updates to Hardware and Software

Once per month, a staff member designated by the executive director shall review that all computer workstations, including portal electronic devices, have the most up-to-date version of the respective operating system, browsers, and security software, and that only whitelisted apps have been installed, and that all security settings and features meet the appropriate security thresholds. Any non-compliance should be addressed and corrected during this monthly review.

Updates to hardware are only to be performed by employees or technicians authorized by the executive director, and hardware components that are being retired must only be disposed of with the approval of the executive director, and in a manner that ensures that the hardware's former data is irrecoverable.

End of Day Procedures

At the end of each day, the last employee leaving the office must:

1. Ensure that all windows and blinds are closed.
2. Ensure that computer monitors are turned off.
3. Ensure that computers and printers are placed in 'sleep' or 'hibernate' modes.
4.
5. Ensure that all secure doors, cabinets, etc., are locked.
6. Set the alarm on the way out of the office.

"Clean Desk" Protocol

Personal information must never be left unattended and exposed at employees' workstations. This includes when shifts are being worked at the desk in the Members Centre. In order to protect personal information in our custody, our employees, board members, and volunteers must:

1. Lock computer workstations when leaving them unattended, even if only for a few minutes.
2. Ensure that records containing personal information are not left unattended on desks.

3. Ensure that superseded or unnecessary records are securely shredded, rather than recycled.

Traveling

When traveling with devices containing personal information held by the Capilano Students' Union, employees, board members, and volunteers are expected to ensure that personal information is safeguarded with appropriate security measures, including password protection and device encryption. Lost or stolen devices must be reported to the privacy officer right away. Devices should not be loaned to any person other than the authorized user for any reason if personal information might be accessed.

Portable Storage Media

If portable storage media (such as a USB key) must be used, only storage media owned by the Capilano Students' Union should be used for records containing personal information. Before that portable storage media is discarded or transferred to another person, it must be securely erased/formatted.

On a permanent Mac workstation in the office:

1. Open Disk Utility.
2. Select the volume to securely erase (e.g., a USB key).
3. Under the 'erase' heading, select 'security options.'
4. Select the option that 'writes a single pass of zeros over the entire disk.'

G Suite Administrators

In order to protect the personal information of our board members, employees, Capilano Students' Union members, and members of the public, access to the information that we hold electronically is provided only to those employees who have an operational need to access the information. The executive director assigns these roles, and monitors these permissions on a monthly basis.

Super Administrators

These users have full permissions across all of the organization's G Suite administrative controls, including control over setting up and applying settings to organizational structures, creating and removing users, managing user and domain security, creating and changing groups, editing the domain registration, using usage reports and audit logs, access Google Cloud support, and activate/deactivate services; these are also the only users who can change other users' administrative privileges:

- executive director
- director, communications and marketing

Groups Administrators

These users have full permissions to create, modify, and remove groups (which function like email distribution lists – such as campaigns@csu.bc.ca, which contains the employees and board members who attend campaigns and advocacy committee meetings):

- resource staff

User management administrator

These users have full permissions to view user profiles, create and delete user accounts (except for other administrator accounts), rename users and change passwords, manage a user's individual security settings, and a few other tasks related to individual users:

- resource staff

Board resources administrator

These users have been granted custom permissions to manage the Google Calendar service, to migrate files and folders between My Drive and Team Drives, and to approve templates submitted by users, and to manage the Google Directory (i.e., the internally-shared, up-to-date list of csu.bc.ca contacts):

- resource staff

Privacy Breach Response

In the event that someone becomes aware of a privacy breach (or a potential privacy breach), the person who becomes aware of the breach (or potential breach) must report the details of the situation to the executive director immediately. Upon becoming aware of a breach (or a potential breach), the executive director shall coordinate the organization's response using the following four-step process.

Response and containment

1. The breach (or potential breach) must be reported to the executive director.
2. The executive director must assess whether a breach has occurred and, if so, to what extent.
3. Immediate corrective actions must be taken to contain the breach.
4. The executive director must thoroughly document the details of the situation.
5. A brief must be prepared to advise the privacy commissioner's office, including:
    a. Nature and scope of the breach;
    b. Steps already taken, and steps that are going to be taken to manage the breach;
    c. Plans to notify affected individuals and third parties; and
    d. Timeframe for providing the board/executive with updates on the situation.

Notification

1. The executive director must prepare a notification to the affected parties, including:
    a. What happened and when;
    b. A generic description of the personal information that was compromised;
    c. Potential or actual risks of harm raised by the breach;
    d. Actions taken to address the situation; and
    e. Any actions that the individual should take to protect themselves.
2. The executive director must ensure that the following guidelines are observed:
    a. Ensure that notification only happens once the facts are confirmed;
    b. Ensure that notice is sent to the correct recipient(s);

c. Communicating with a representative if someone cannot receive a notification;
d. Ensuring that a script is used for notifications by telephone; and
e. Ensuring that letter notifications are clear, concise, and accurate.

Investigation

1. The executive director must investigate the events that led to the privacy breach.
2. The executive director must evaluate the steps taken to contain the breach.
3. The executive director must recommend remedial actions to prevent future breaches.

Implementation of changes

1. The executive director must coordinate the implementation of improved prevention strategies.
2. A meeting should be held with all parties involved in the breach to determine steps forward.
3. The execution of remedial actions should include the following:
    a. Reviewing existing information management systems;
    b. Amending or reinforcing existing privacy policies and procedures;
    c. Development and implementation of new security and privacy measures;
    d. Training the team on legislative requirements, and privacy policies/procedures; and
    e. Testing and evaluation of remedial actions to ensure effectiveness.

Document Retention

In order to ensure that the Capilano Students' Union can meet certain legal obligations and operational needs, sensitive records must be retained for certain periods of time before they can be discarded. Once these retention periods have expired, to ensure that the personal information of individuals is protected, these sensitive records are securely destroyed.

Once a sensitive record's retention period has expired, the document should be separated from other active records and shredded. The document must not be unattended at any time between its removal and its destruction.

Document type	Retention period
Human resources records	
Résumés and competition records Solicited résumés and application packages for posted vacancies, and interview notes; we do not have a requirement to keep unsolicited application packages.	1 year Exception: 6 years for records that could become the subject of a discrimination complaint.
Personnel file Includes correspondence, evaluations, contracts, reports on vacation and leave, and adverse reports.	6 years (after employment ends)
Payroll records Includes any reports mandated to be kept under section 28(1) of the *Employment Standards Act*.	6 years

Records of Employment (ROEs) (employer copy)	6 years
Health and safety records	
WorkSafeBC records Includes first aid logs and incidents, accident investigations, and ergonomic risk assessments.	10 years
Governance records	
Board minutes	Permanent
Committee minutes	10 years
Constitution and bylaws	Permanent
Financial records	
General ledger	Permanent
Financial statements (annual)	Permanent
Records for endowment donations	Permanent
Records for long-term acquisitions	Permanent
Financial statements (monthly)	6 years
Cheques – cancelled	6 years
Cheque stubs	6 years
Bank statements	6 years
Invoices (accounts receivable)	6 years
Bills (accounts payable)	6 years
Bank reconciliations	6 years

	Procedure Name	Approval Authority
	**Privacy Procedures**	Executive Director
	Created Under	**Approval Date**
	Privacy Policy	**August 18, 2017**
	Responsible	**Scheduled Review**
	Executive Director	August 2018

Event records	