LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA POLICY MANUAL	
SECTION	Members' Policies
POLICY	7410 – Appropriate Use of IT Resources for Members and Employees of a Member or Caucus

Objective

To ensure that information technology resources are used appropriately to protect the privacy, confidentiality, and security of Legislative Assembly information, including information under the control of a Member of the Legislative Assembly, and the protection of Legislative Assembly assets.

Application

This policy applies to Members of the Legislative Assembly and to employees, volunteers, and contractors under the direction of a Member or caucus.

Authority

Policies affecting Members of the Legislative Assembly are approved by the Legislative Assembly Management Committee, as per *Policy 1000 – Legislative Assembly Policy Framework*.

Key Definitions

"**device**" means any electronic computing or communication technology, including, but not limited to computers, laptops, tablets, smartphones, telephones, printers, monitors, and headsets;

"**ITD**" refers to the department of the Legislative Assembly Administration responsible for information technology;

"**IT resource"** means all information and communications technologies including, but not limited to apps, software, devices, peripherals, and information storage;

"**Legislative Assembly IT resource**" means an IT resource that is an asset of the Legislative Assembly, which includes any devices, peripherals, apps and software licences allocated or managed by the ITD or purchased or developed with Legislative Assembly funds, and IT resources owned, licensed, or managed by the ITD such as the Legislative Assembly network, information systems and storage, and its related equipment, hardware, and peripherals;

"**sensitive information**" means information that is not public and that, if compromised, could cause injury to a person, a Member, or the Legislative Assembly;

"**supervisor**" refers to the Member or the caucus employee responsible for the oversight of an employee, volunteer, contractor, or other user;

"**user**" means a person who uses a Legislative Assembly IT resource, including a Member and an employee, volunteer, or contractor under the direction of a Member or caucus.

1. General

.01 As users of IT resources, Members and employees of a Member or a caucus play an essential role at all times in ensuring the appropriate use of Legislative Assembly resources, privacy, confidentiality and security of information, and the efficient operation, integrity, and security of Legislative Assembly IT resources.

.02 A user must submit all requests and reports under this policy to the ITD in writing using the Service Desk User Portal accessible via the Legislative Assembly's intranet or via email to ServiceDesk@leg.bc.ca.

2. Responsibility Overview

.01 A user is responsible for ensuring that they are aware of their responsibilities under this policy and seeking clarity from the ITD if there is uncertainty. A user must:

a) use reasonable care while handling a Legislative Assembly IT resource to protect against avoidable physical damage;
b) protect Legislative Assembly information from unauthorized access by locking their screen when a device is unattended and ensuring that their screen is not visible to unauthorized persons; and
c) only store Legislative Assembly information on an IT resource that is supplied by the ITD or has been otherwise approved for use.

.02 A supervisor is responsible for managing a user's access rights to Legislative Assembly IT resources and Legislative Assembly information (e.g., requesting access rights for a new user or requesting a change to access rights if there is a change to a user's role). A supervisor must:

a) ensure that a user under their direction is aware of their responsibilities as set out in this policy;
b) ensure the user is provided the minimum level of access to Legislative Assembly IT resources and Legislative Assembly information required to conduct their work and that access is not an automatic entitlement based on status, rank, or office (i.e., the principle of least privilege);

c) review user access for the principle of least privilege on an annual basis, at a minimum; and
d) notify the ITD within 60 days when an employee, volunteer, or contractor relationship ends to terminate user access and if desired, archive user account data.

.03 The ITD is responsible for monitoring, in the context of identifying threats to security or efficient operation, the activity of IT resources that access the Legislative Assembly network or information systems and maintaining procedures on managing user access. Should the ITD detect a threat to the security or efficient operation of Legislative Assembly IT resources, the ITD may:

a) limit, remediate, or isolate user access;
b) suspend or restrict user access to Legislative Assembly IT resources; and
c) block user installation or access to apps and software on Legislative Assembly IT resources and support a user with alternative solutions.

3. Use of Legislative Assembly IT Resources

.01 A user is provided personalized access rights to use Legislative Assembly IT resources and access Legislative Assembly information (e.g., email, Microsoft Teams, Maximizer, enterprise resource planning system). The ITD is responsible for providing Members and supervisors with information to support appropriate user access rights and managing user access rights at the direction of the user's supervisor.

.02 A user must use their own access rights and must not share access without approval from the ITD. For example, if a user wishes to delegate temporary access to an information system (i.e., temporary access to Maximizer while a user is away), or if an app or software does not permit unique access credentials, the user must document the request in writing to the ITD and the user must implement any mitigating controls directed by the ITD.

.03 A user must not share or compromise the authentication information they use to access Legislative Assembly IT resources (passwords, mobile and tablet personal identification numbers (PINs), access cards, etc.). A user must not:

a) share authentication information;

b) write or otherwise store authentication information in unauthorized digital applications or physical locations; or
c) reuse Legislative Assembly authentication information elsewhere (e.g., using a Legislative Assembly password as a personal social media account password).

.04 A user must use Legislative Assembly provided accounts (e.g., email and file storage) when conducting Legislative Assembly business. For certainty, a Member may use an account issued by the Government of British Columbia when conducting business as part of, or on behalf of, the Executive Council.

.05 Auto forwarding a Legislative Assembly email account to an account outside of the Legislative Assembly email system is prohibited.

4. Use Outside of Canada

.01 When planning to access or take Legislative Assembly IT resources outside of Canada, a user must advise the ITD in advance, with as much notice as possible, to ensure that they will have functional access without jeopardizing the integrity of Legislative Assembly IT resources or Legislative Assembly information.

.02 A user must comply with any mitigations required by the ITD to access Legislative Assembly IT resources outside of Canada.

5. Permitted Personal Use

.01 Reasonable personal use of Legislative Assembly IT resources is permitted provided it is lawful, in line with applicable workplace conduct policies and agreements applicable to the user, and:

a) does not compromise the reliability and security of Legislative Assembly IT resources or Legislative Assembly information, specifically personal or sensitive information;
b) is not used for political party or electoral activities; and
c) is not used for personal gain.

.02 The Legislative Assembly is not responsible for the loss of any personal data saved on a Legislative Assembly IT resource. To protect privacy, ensure efficient use of storage, and mitigate personal data loss, a user should avoid storing personal data on a Legislative Assembly IT resource.

6. Non-Legislative Assembly Devices

.01 If a user wishes to access Legislative Assembly IT resources or Legislative Assembly information via a device not supplied by the ITD,

such as a personal device, public device, or Government of British Columbia issued device:

a) the user must use multi-factor authentication; and
b) the user must use security technology provided by the ITD.

.02 Access to Legislative Assembly information from a non-Legislative Assembly device is conditional. The ITD may limit, remediate, or isolate user access if the ITD assesses the device, or user activity on the device, is a risk to the operation, integrity, or security of Legislative Assembly IT resources or Legislative Assembly information.

7. Prohibited Use

.01 Use of Legislative Assembly IT resources for the following activities or purposes is prohibited:

a) any activity that may expose a Member, an employee of a Member or a caucus, or the Legislative Assembly to legal liability;
b) deliberately introducing malware, a virus, or other malicious software code;
c) disabling or deliberately tampering with security protection software or controls;
d) directing or engaging in an activity that involves unauthorized access to or collection of personal or sensitive information;
e) engaging in an activity that has a commercial purpose or for the purpose of solicitation, advertising, or personal financial gain, including online gambling;
f) misappropriating or infringing on the patent, copyright, trademark, or other intellectual property rights of any third party, including copying material from a third party (including text, graphics, music, videos, or other copyrightable material) without proper authorization;
g) bullying, harassment, or actions in violation of any applicable respective workplace conduct policy and agreement for any user;
h) viewing, downloading, or communicating defamatory, discriminatory, violent, obscene, or otherwise inappropriate content unless required in the course of the user's work;
i) violating any applicable procedures, policies, or laws; and
j) any other purpose deemed inappropriate and communicated by the Chief Information Officer due to adverse implications

for the reliability or security of Legislative Assembly IT resources or Legislative Assembly information.

8. Monitoring and Compliance

.01 Any suspected or actual breach of this policy must be reported without delay as follows:

User	Report To
Speaker of the Legislative Assembly	Chief Information Officer
Member affiliated with a caucus	Chief Information Officer and Caucus Chair (or the House Leader if the Member is the Caucus Chair)
Member unaffiliated with a caucus	Chief Information Officer
Employee, volunteer, or contractor under the direction of a Member	Chief Information Officer and Member
Employee, volunteer, or contractor under the direction of a caucus	Chief Information Officer and Caucus Executive Director or Chief of Staff; or Caucus Chair in the event the user is the Caucus Executive Director or Chief of Staff

.02 The Director of the ITD or their designate will review any reported or suspected breach of this policy. A review may include, but is not limited to, the search and seizure of Legislative Assembly IT resources without notice to the user under review.

.03 A user must cooperate with a review when requested to do so.

.04 If the Director of the ITD assesses the suspected breach of policy to be intentional or to have compromised the security of Legislative Assembly IT resources or Legislative Assembly information, the Chief Information Officer or their designate will review the facts and any available information or evidence concerning the allegation and determine if further action or investigation is warranted.

.05 If an allegation warrants action or investigation, the Chief Information Officer or their designate, must:

a) seek the advice of the Law Clerk and Parliamentary Counsel or their designate; and
b) notify in accordance with the table below:

User	Notify
Speaker of the Legislative Assembly	Subcommittee on Administration and Operations of the Legislative Assembly Management Committee
Member affiliated with a caucus	Caucus Chair (or the House Leader if the Member is the Caucus Chair)
Member unaffiliated with a caucus	Speaker of the Legislative Assembly
Employee, volunteer, or contractor under the direction of a Member	Member
Employee, volunteer, or contractor under the direction of a caucus	Caucus Executive Director or Chief of Staff; or Caucus Chair in the event the user is the Caucus Executive Director or Chief of Staff

.06 If a user fails to cooperate in an investigation, the Chief Information Officer or their designate may refer the matter to the Subcommittee on Administration and Operations of the Legislative Assembly Management Committee for consideration.

.07 The Chief Information Officer, or a person designated by the Clerk of the Legislative Assembly, may use the services of a third party and may securely transfer any seized Legislative Assembly IT resources to a third party for the purpose of completing an investigation.

.08 The Chief Information Officer or their designate must report the findings of an investigation and any subsequent corrective measures to the appropriate person or entity listed in section 8.05. If the Chief Information Officer or their designate determines that a user has contravened this policy, the user will be informed about the outcome of the review and any subsequent corrective measures prescribed by the ITD.

.09 The Chief Information Officer or their designate may implement corrective measures for a user found to have contravened this policy. Corrective measures will depend on the nature of the policy breach and threat to the security of Legislative Assembly IT resources or Legislative Assembly information (e.g., user training, restrict user access to Legislative Assembly IT resources).

.10 In the event of a dispute with respect to the prescribed corrective measures or continued non-compliance, the Chief Information Officer or their designate may refer the matter to the Subcommittee on Administration and Operations of the Legislative Assembly Management Committee for consideration.

.11 The Chief Information Officer may, at their sole discretion, refer a contravention of this policy that exposes the Legislative Assembly to significant risk to the Subcommittee on Administration and Operations of the Legislative Assembly Management Committee for consideration.

Contact Please contact the ITD Service Desk with any questions regarding this policy at ServiceDesk@leg.bc.ca.

Approved and authorized by the Legislative Assembly Management Committee on May 7, 2024.

POLICY HISTORY	
Version 1	May 7, 2024