LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA POLICY MANUAL	
SECTION	Information Management / Information Technology
POLICY	5405 – Appropriate Use of Information Technology Resources

Objective

To ensure that information technology resources are used appropriately to protect Legislative Assembly assets and the privacy, confidentiality, and security of the Legislative Assembly's information.

Application

This policy applies to all employees of the Legislative Assembly appointed under section 39 of the *Constitution Act* (R.S.B.C. 1996, c. 66) and may also apply, in part or in full, to contractors when required by their contractual agreement with the Legislative Assembly.

Authority

Legislative Assembly operational policies are approved by the Clerk of the Legislative Assembly, as per *Policy 1000 – Legislative Assembly Policy Framework.*

Key Definitions

"**AI tool**" means any technology that uses AI to perform a specific task;

"**artificial intelligence**" or "**AI**" means technology that can produce outputs that may appear to have been created by a human such as content, predictions, recommendations, or decisions that influence the environments with which it interacts;

"**confidentiality**" means the principle that information is not made available or disclosed to unauthorized individuals or entities;

"**data**" means raw material such as facts or figures stored in a structured manner that, given context, turns into information or transactions contained in information systems, applications, and databases;

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

"generative AI" means a type of artificial intelligence that generates new content (e.g., text, images, code, audio, or video) in response to inputs;

"**information**" means representations of facts, ideas, and opinions on subjects, events, and processes, regardless of medium or format, including data contained in IT resources;

"**information incident**" means a single or series of events involving the collection, storage, access, use, disclosure, or disposal of

Legislative Assembly information that threatens privacy or information security or contravenes law or policy;

"**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;

"personal information" means recorded information about an identifiable individual that is not business contact information (name, position name or title, business telephone number, business address, business email, or business fax that enables an individual to be contacted at a place of business);

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

"supervisor" means the person the employee directly reports to.

1. General

.01 As users of IT resources, employees play an essential role 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 An employee must comply with *Policy 4015 – Standards of Conduct* when using IT resources, whether use is related to their employment duties or permitted incidental personal use.

.03 A contractor provided with a Legislative Assembly device or account must follow the requirements of this policy as set out for an employee when using a Legislative Assembly IT resource.

2. Responsibility Overview

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

a) use reasonable care while handling a Legislative Assembly IT resource to protect against avoidable physical damage;
b) only store Legislative Assembly information on IT resources that are supplied by, or otherwise approved for use by, the ITD;
c) seek advice from the ITD to protect Legislative Assembly information by encrypting if stored on a removable media device and ensure that the device is not shared;
d) ensure Legislative Assembly information is not stored on the local disk of a device for longer than necessary for processing, as it is not subject to the Legislative Assembly's backup solutions;
e) protect Legislative Assembly information from unauthorized access by locking screens when devices are unattended and by ensuring that screens are not visible to unauthorized persons; and
f) use emerging technologies (e.g., generative AI) in accordance with guidance and directives issued by the Legislative Assembly.

.02 An employee responsible for purchasing or procuring services from a contractor must consider which elements of this policy are appropriate to be formalized in the contract. Pursuant to *Policy 3105 – Contracting*, the ITD must be consulted in the preparation of a contract if a contractor requires access to a Legislative Assembly IT resource. The employee must ensure that a contractor developing or implementing a new AI tool for the Legislative Assembly meets the requirements of the *Procedure on the Integration of AI*.

.03 A supervisor must:

a) ensure that an employee is aware of their responsibilities as set out in this policy;
b) ensure the employee 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 employee access for the principle of least privilege on an annual basis, at a minimum; and

d) notify the ITD within 30 days when an employee or contractor relationship ends or changes to terminate or update user access.

3. Use of Legislative Assembly IT Resources

.01 An employee must use Legislative Assembly-provided accounts (e.g., email and file storage) when conducting Legislative Assembly business.

.02 Auto-forwarding a Legislative Assembly communications account (e.g., Microsoft Teams, Outlook) to a communications account outside the Legislative Assembly system is prohibited.

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

a) share authentication information, including by sharing passwords with the IT Service Desk or other technical support staff;
b) write or otherwise store authentication information in unauthorized digital applications or physical locations; or
c) reuse Legislative Assembly authentication information elsewhere (e.g., use a Legislative Assembly password as a personal social media account password).

.04 Delegated access to Legislative Assembly IT resources on behalf of an employee must be documented in writing and utilize separate access rights, rather than the sharing of access credentials, where possible. Where a software application does not permit unique access credentials, an exception must be requested in accordance with section 8.02.

4. Use of Legislative Assembly IT Resources Outside of Canada

.01 When planning to use a Legislative Assembly IT resource outside of Canada (e.g., using a Legislative Assembly device, logging in to a Legislative Assembly account through a personal device), the employee or their supervisor must advise the IT Service Desk in advance, with as much notice as possible, to ensure that the resource will be fully functional without jeopardizing the integrity of Legislative Assembly IT resources or Legislative Assembly information. Legislative Assembly IT resources will not function outside of Canada without ITD authorization.

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

5. Use of Artificial Intelligence (AI)

.01 The use of AI is subject to the following:

a) ***Procedure on the Integration of AI***
The *Procedure* establishes requirements for integrating AI tools into Legislative Assembly information assets, principles for approving an AI tool, risk classification, and governance for implementing and managing AI tools. The ITD must review the *Procedure* at minimum quarterly to ensure appropriate risk management of evolving technology and amendments must be authorized by the Chief Information Officer; and

b) ***Guide to Using Generative AI***
The *Guide to Using Generative AI* provides guidance for employees on best practices, personal and sensitive information input, content review, disclosure of use, and employee responsibility. Amendments to the *Guide to Using Generative AI* must be authorized by the Chief Information Officer and the Law Clerk and Parliamentary Counsel.

.02 The use of AI tools must uphold the values of the Legislative Assembly Administration (as set out in the Strategic Plan) and the protection of information. An employee remains fully responsible for the accuracy, completeness, and appropriateness of all work, whether or not an AI tool was used.

.03 Generative AI is a decision-support tool only and must not be used for autonomous decision-making or to generate official records without human review and approval.

.04 When using non-public Legislative Assembly information or completing work-related tasks, an employee must only use AI tools that have been approved by ITD. When using these tools, an employee must:

a) follow any directions issued by ITD on using that AI tool;
b) follow the *Guide to Using Generative AI*;
c) review all outputs from the AI tool to ensure they are accurate, complete, and appropriate (e.g., use a professional tone, use inclusive language); and

d) disclose when the substantive basis of their content, analysis, or recommendations has been produced by generative AI.

.05 ITD will maintain an inventory of sanctioned and unsanctioned AI tools. When deciding whether to approve a tool, ITD must:

a) consult with Legal Services;
b) review the tool in line with the *Procedure on the Integration of AI* to determine whether it supports the safe, secure, and privacy-conscious handling of Legislative Assembly information; and
c) document the justification for its decision.

The Director of the ITD is responsible for approving sanctioned AI tools. When approving the use of an AI tool, ITD may impose restrictions as part of that approval. For instance, ITD may approve a tool for use only by specific teams for specific purposes and with specific safeguards in place.

.06 ITD or the director of a department developing an AI tool sanctioned by the ITD may monitor the AI tool to ensure it is used responsibly and follows the best practices outlined in AI guidance issued by ITD. ITD may limit or withdraw approval of any AI tool if it no longer meets these standards.

.07 ITD will provide training and guidance to help employees use AI effectively and build AI literacy. In some cases, the director of the department managing an AI tool may require employees in specific roles to complete AI training to ensure safe, responsible, and informed use of that tool.

.08 An employee or team developing or implementing a new AI tool must follow the *Procedure on the Integration of AI*. Where the development of an AI tool will be contracted to a third party, the contractor must meet the requirements of the procedure.

.09 The director responsible for the department managing an AI tool must ensure the AI tool is reviewed at least every 2 years to ensure ongoing risk management in relation to security and privacy.

6. Recording and Transcription

.01 To protect personal privacy, the recording of meetings (in-person, virtual, or hybrid) using an IT resource is limited. A meeting may be

recorded by an employee, with advance notice to all meeting participants, for the following purposes:

a) training; or
b) providing a reliable record to assist with drafting meeting minutes.

.02 Generative AI transcription may be used for meetings, with advance notice to all meeting participants, for the following purposes:

a) supporting accessibility by ensuring equitable understanding of meeting content; or
b) enabling efficient meeting summaries to be prepared.

Any transcription produced through generative AI should be disposed of as soon as practicable.

.03 Recordings of confidential or unpublished Legislative Assembly content must be stored using Legislative Assembly IT resources whose data remains in Canada.

7. Permitted Personal Use

.01 Reasonable personal use of Legislative Assembly IT resources is permitted provided it is lawful, in line with *Policy 4015 – Standards of Conduct*, and:

a) is limited during core business hours and does not interfere with the employee's duties and responsibilities;
b) does not compromise the reliability and security of Legislative Assembly IT resources or Legislative Assembly information, specifically personal or sensitive information; 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, an employee should avoid storing personal data on a Legislative Assembly IT resource.

8. Prohibited Use

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

a) any activity that may expose an individual or the Legislative Assembly to legal liability;

b) deliberately introducing malware, viruses, or other malicious software code to a device or the network;
c) disabling or deliberately tampering with security protection software or controls;
d) directing or engaging in activities that involve unauthorized access to or collection of personal or sensitive information;
e) bullying or harassment;
f) viewing, downloading, or communicating defamatory, discriminatory, violent, obscene, or otherwise inappropriate content unless required in the course of the employee's work;
g) engaging in activities that have a commercial purpose or for the purposes of solicitation, advertising, or personal financial gain, including online gambling;
h) misappropriating or infringing on the patent, copyright, trademark, or other intellectual property rights of any third party, including copying material from third parties (including text, graphics, music, videos, or other copyrightable material) without proper authorization;
i) violating any applicable procedures, policies, or laws; and
j) any other purpose deemed inappropriate by the Chief Information Officer due to adverse implications for the reliability or security of Legislative Assembly IT resources or Legislative Assembly information.

.02 The Director of the ITD may approve exemptions to section 2.01, section 3 "Use of Legislative Assembly IT Resources" and section 8 "Prohibited Use". An employee seeking an exemption must submit their request in writing, including the reason for the request. The Director of the ITD will consider the request based on business need and any alternative options. If the request is approved, the employee must comply with any mitigations required by the ITD. The Director of the ITD is responsible for tracking exemptions.

9. Monitoring and Compliance

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

Employee	Report To
Clerk of the Legislative Assembly	Chief Information Officer
Member of the Clerk's Leadership Group	Chief Information Officer

Chief Information Officer	Clerk of the Legislative Assembly
Director of the ITD	Chief Information Officer
All other employees	Director of the ITD and Supervisor

.02 If the employee suspected to have breached the policy is the Chief Information Officer, the Clerk of the Legislative Assembly will designate another individual to perform the responsibilities assigned to the Chief Information Officer in this section.

.03 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 individual under review. Review is restricted to Legislative Assembly apps and accounts, whether they are on a Legislative Assembly device or a personal device.

.04 An employee must cooperate with an investigation when requested to do so.

.05 The Director of the ITD will share the findings of their review with the Chief Information Officer. The Chief Information Officer must review the facts and any information or evidence that is available in serving as the basis of the allegation when determining the merits of initiating an investigation.

.06 If an allegation warrants action, prior to initiating an investigation, the Chief Information Officer must, except in urgent situations where immediate action is necessary:

a) seek the advice of the Law Clerk and Parliamentary Counsel and the Chief Human Resources Officer, as appropriate; and
b) obtain the approval of the person listed in the table below:

Employee	Approver
Clerk of the Legislative Assembly	Subcommittee on Administration and Operations of the Legislative Assembly Management Committee
Member of the Clerk's Leadership Group	Clerk of the Legislative Assembly

Chief Information Officer	Clerk of the Legislative Assembly
Directors	Member of the Clerk's Leadership Group Responsible for the Department
All other employees	Department Director

.07 The Chief Information Officer must report the findings of the investigation to the person or entity whose approval was sought under section 9.06. If the Chief Information Officer determines that an employee has contravened this policy, the employee will be informed about the outcome of the review and any subsequent corrective measures prescribed by the ITD.

.08 An employee found to have contravened this policy may be required to complete training or may be subject to disciplinary action, including termination for cause, as detailed in *Policy 4050 – Progressive Discipline*. The Legislative Assembly reserves the right to pursue any and all legal remedies available under applicable law in response to any breaches that occur as a result of a violation of this policy.

.09 The Chief Information Officer may use the services of a third party to carry out an investigation and may securely transfer any seized Legislative Assembly IT resources to a third party for the purpose of completing an investigation.

Contact	Please contact the Information Technology Department with any questions regarding this policy at ServiceDesk@leg.bc.ca.
Procedures	*Procedure on the Integration of AI* *Guide to Using Generative AI*
References	***Policy 3105 – Contracting*** ***Policy 4015 – Standards of Conduct*** ***Policy 4050 – Progressive Discipline***

Kate Ryan-Lloyd

Approved and authorized by Kate Ryan-Lloyd,
Clerk of the Legislative Assembly

February 11, 2026

Date

POLICY HISTORY	
Version 1	April 14, 2005
Version 2	March 6, 2017
Version 3	February 2, 2022
Version 4	February 11, 2026