Privacy Impact Assessment
City of Port Moody

Attending Meetings and Accessing Email from Outside of Canada

PIA File #: 2022-004

PART 1: GENERAL INFORMATION

Name of Department/Branch:	Administration Department – Legislative Services		
PIA Drafter:	Tracey Takahashi		
Email:	ttakahashi@portmoody.ca	Phone:	(604) 469-4539
Program Manager:	Tracey Takahashi		
Email:	ttakahashi@portmoody.ca	Phone:	(604) 469-4539

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner. **No**
Is this initiative a common or integrated program or activity? Under section *FOIPPA* 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner. **No**
Related PIAs, if any: **N/A**

1. What is the initiative?

The City would like to enable remote attendance at Council meetings by Council members who are travelling outside of Canada, as well as remote attendance at meetings by City employees who are travelling outside of Canada (council meetings and staff meetings). The City would also like to enable Council members and employees who are travelling outside of Canada to be able to temporarily access their City email accounts and the City server remotely. The intention is for this access to occur in a similar manner as it does from within Canada. This initiative is not intended to permit the disclosure or storage of personal information outside of Canada.

2. What is the scope of the PIA?

The PIA considers and addresses whether there are any privacy risks that arise from enabling temporary access to City email and the City server, as well as electronic attendance at meetings outside of Canada. The PIA is premised on the City's intention not to permit Council or staff

who are travelling outside of Canada to disclose or store any personal information outside of Canada.

3. What are the data or information elements involved in your initiative?

The information that may be accessed or used by Council members and employees remotely outside of Canada is the same that would be accessed by those same individuals from within Canada. The data or information elements cannot be identified in advance with specificity since they will depend on what is being considered at a Council or staff meeting, or what work is being carried out remotely. A summary of the types of data or information is considered below:

(a) Council meetings

Council members and employees who attend meetings outside of Canada will do so via Zoom or Microsoft Teams, which are the same platforms the City already uses to conduct meetings electronically. Council members and employees will not be permitted to record meetings they attend from outside of Canada. During the meetings, they may have access to agendas, staff reports, and other documents, some of which may contain personal information. These records will be accessed on the member or employee's own device (laptop, iPad, or other mobile device) from a private location and will not be stored or otherwise disclosed outside of Canada.

All the information being considered at regular open meetings is information that is or would be publicly disclosable under the *Freedom of Information and Protection of Privacy Act (FIPPA*). Information being considered at closed meetings may not be information that can be publicly disclosable under *FIPPA*. However, the expectation is that if it is being disclosed to Council and staff members, that disclosure is done in accordance with *FIPPA* (i.e., the City has authority under s. 33 of *FIPPA* to disclose the personal information to Council members and staff).

(b) Email accounts

City email accounts are hosted on Microsoft 365 on servers located in Canada. Therefore, even when Council members or staff temporarily access their email outside of Canada, there would be no disclosure or storage outside of Canada. The access would take place on the member or employee's own device in a private location.

Data or information contained in a Council member or employee's email account may include personal information. However, the expectation is that this would be information that the Council member or employee is entitled to have access to under *FIPPA* (whether they are physically located in Canada or outside of Canada while accessing the information). There is nothing specific about this initiative that requires the disclosure of additional personal information beyond that which would normally be accessed while performing work in Canada.

(c) Other City Records

Council members and staff may access personal information on the City server (along with information and records that are not necessarily personal or confidential). They would be entitled to access the same information from within Canada for the purposes of carrying out their duties, powers, and functions.

The City already has protections in place to ensure that access to confidential or private City records is restricted to only those employees who require access in order to perform their

duties. For example, employees do not have access to in-camera documents unless they are granted specific permission by Legislative Services. Permission would only be granted in accordance with *FIPPA*.

3.1 Did you list personal information in question 3?

Yes.

4. How will you reduce the risk of unintentionally collecting personal information?

This initiative does not specifically require the collection of personal information from employees or Council members. The only information that might be collected by the City is metadata showing when Council members or employees may have accessed the City's server (which is information that would be collected inside of Canada as well). However, we do not think there is any risk of Council members or employees unintentionally collecting personal information simply by attending meetings and accessing City records in the course of carrying out their duties outside of Canada.

Council members and employees will be required to attend meetings and otherwise perform their duties and functions from a private location while they are outside of Canada (such as a private hotel room or private Airbnb). They will also be required to use their own private device.

PART 2: COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION

5. Collection, use, and disclosure

Ways Personal Information might be accessed	**Collection, use, or disclosure**	***FOIPPA* authority**	**Other legal authority**
During Council/staff meetings: Council meetings are on Zoom. Staff meetings are typically on Microsoft Teams. Council members (and staff attendees) would access in-camera agendas and other records via email (hosted by Microsoft 365 on servers in Canada) or via eScribe (a service used for agenda management, also hosted in Canada). Identities of meeting attendees are authenticated through email accounts to ensure there are no unauthorized attendees at in-camera meetings.	If personal information is involved, it would be access/disclosure (but only temporary disclosure to the member or employee in question).	The City would ensure *FIPPA* compliance prior to disclosure. The specific authority would depend on what the personal information is, but likely s. 33(2)(b), (d), (e), (f), or (h).	
Through City Email: Access by Council members and employees outside of Canada would be in the same manner as email would be accessed if the Council member or employee was working remotely from inside Canada. Password authentication is required.	Temporary access/disclosure.	Depends on what the personal information is, but likely s. 33(2)(b), (d), (e), (f), or (h).	

Ways Personal Information might be accessed	Collection, use, or disclosure	*FOIPPA* authority	Other legal authority
Through the City's Server: Access by Council members and employees while outside of Canada would be through the same mode while in Canada. Access requires password authentication. Everything is restricted to a 'need only' basis.	Temporary access/disclosure.	Depends on what the personal information is, but likely s. 33(2)(b), (d), (e), (f), or (h).	

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

6. Is any personal information stored outside of Canada?

No. Council members and employees may temporarily access personal information electronically while they are carrying out their duties from outside Canada, but it is not permitted to be stored by employees or Council members outside of Canada.

7. Does your initiative involve sensitive personal information?

The initiative does not involve the storage, use, or disclosure of sensitive personal information outside of Canada. In no circumstance will a Council member or employee be permitted to take sensitive personal information with them (in hard copy) outside of Canada. In no circumstance will a Council member or employee be permitted to record a meeting at which sensitive personal information is discussed.

8. Is the sensitive personal information being disclosed outside of Canada under *FOIPPA* section 33(2)(f)?

No.

9. Where are you storing the personal information involved in your initiative?

Any personal information that would be available to Council members or employees would be stored on the City's servers (in Canada).

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer. More help is available in the Guidance on Disclosures Outside of Canada.

10. Is the sensitive personal information stored by a service provider?

The City does not intend to store any personal information outside of Canada as part of this initiative. All City records and email accounts are stored in Canada.

11. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A

12. Does the contract you rely on include privacy-related terms?

N/A

13. What controls are in place to prevent unauthorized access to sensitive personal information?

Accessing City email is password protected with Microsoft's multi-factor authentication. This requires the user when not working onsite to have the Microsoft app on an iPhone to approve the access. Accessing data remotely through the VPN system is password and multifactor authenticated with DUO and is similar. The user needs to be able to confirm from a secondary device that they are approving the login, before allowing any access internally. Our password systems policy requirements are to change the password every 90 days, with minimum seven (7) characters and users cannot use any of their previous 18 passwords.

Within the server, employees are restricted from accessing all records and only have access to records required for them to perform their duties and functions. This restriction is a membership group done through a security access-control list (ACL), which is a list of permissions associated with the file and folder structure. An ACL specifies which users are granted access to files.

14. Provide details about how you will track access to sensitive personal information.

Our records management system, OpenText provides an audit trail of user file involvement. It will show which user accessed it, on what date, at what time, and whether there was a change to the file.

15. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

The City does not intend to disclose personal information outside of Canada as part of this initiative, beyond the immediate "disclosure" to the Council member or employee (which is just temporary access). Nonetheless, privacy risks have been identified in the following table.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure, or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (This may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk?** **If yes, please describe.**
Council members and employees take hard copies of records with them	Depends on what personal information is contained on the records	Low. This will be prohibited under the Policy and there would be consequences for a breach.	Low	Policy barrier mitigates the risk of this occurring. The policy will also include notification requirements so that any breach may be addressed immediately.	No
Council members or employees attend meetings from a public location while outside of Canada	Depends on what personal information is discussed	Low. This will be prohibited under the Policy and there would be consequences for a breach.	Low	Policy barrier mitigates the risk of this occurring.	No
A device is hacked, or a password is inadvertently disclosed, and access is provided to unauthorized third parties	Depends on what personal information is discussed	The risk is the same as it is at present in Canada	Same risk that is present in Canada	Immediately, upon first detection we reset the device owner's password. We then do a complete wipe and reinstallation of the operating system to get it to a clean state. Depending on the severity, we look into user and firewall logs associated with the device.	No

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

16. Does your initiative involve digital tools, databases, or information systems?

Yes, but the same tools, databases and information systems that are currently being used by the City. The only distinction is that systems may be accessed from outside of Canada.

17. Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of *FOIPPA* section 30?

There will be no specific assessment. The City already has measures in place to prevent unauthorized access to its systems.

18. What technical and physical security do you have in place to protect personal information?

Our digital records are stored centrally at City Hall, and backups of that information are stored at a remote location and encrypted. For our remote users, data on our surface computers are encrypted and password protected at the bios level. All closets and telecommunication rooms are either physically locked or pass key coded.

The City has a dual firewall configuration that blocks all unauthorized traffic. Any data that gets through the firewall is further screened for additional malicious activity and can be automatically acted on by the firewall immediately to remediate the event. This screening process involves the system analyzing the traffic and shutting down the connection if it detects nefarious application in use. In conjunction, we have antivirus software running on all windows servers and computers that provides another security layer by analyzing known threats and either deleting or alerting us of the security event. The remote sites, which include Firehall 2, Kyle Centre, and Carpentry Shops, connect back to City Hall by a secure AES128 encrypted channel. These remote sites share security enabled events and benefit from all other security features of the main branch.

We also have DNS internet filtering system in place that prevents web access to all internal devices to known blacklist and other potential harmful sites. These websites are known as phishing sites created to steal user passwords and other confidential information.

19. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	X
Employees that need standing or recurring access to personal information must be approved by executive lead	X
We use audit logs to see who accesses a file and when	X
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

20. How will you make sure that the personal information is accurate and complete?

There is no personal information that is specifically collected pursuant to this initiative. This initiative merely enables access to the same personal information that would otherwise by accessed by Council members or employees while inside of Canada.

21. Requests for correction

FOIPPA **gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.**

1.1 Do you have a process in place to correct personal information?

N/A on this initiative.

2.1 Sometimes it's not possible to correct the personal information. *FOIPPA* requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A on this initiative.

3.1 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, *FOIPPA* requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A on this initiative.

22. Does your initiative use personal information to make decisions that directly affect an individual?

No.

PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

23. Will your initiative result in a personal information bank?

No.

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

24. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

N/A on this initiative.

PART 9: SIGNATURES

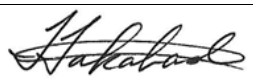
You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

The information contained in this PIA has been reviewed and approved.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Tracey Takahashi		July 11, 2022

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate (if required)			