CITY OF VICTORIA

Privacy Impact Assessment

Victoria Fire Department Mobile Phones

PIA# 2015-008

Part 1 – General

Name of Department/Branch:	Victoria Fire Department, Finance – Information Technology		
PIA Drafters:	Katherine Wilson		
Email:	kwilson@victoria.ca	Phone:	250.361.0392
Program Manager:	Dan Atkinson, Deputy Chief, Operations		
Email:	datkinson@victoria.ca	Phone:	250.920.3356

1. Description of the Initiative

The Victoria Fire Department (VFD) equipped all six front line apparatus with Sonim Smart mobile phones. These phones were selected because they are durable, reliable and easy to use in difficult environments such as fire-fighting.

These devices were procured to enable staff to place private calls "off-air", research relevant topics via the internet, and to allow staff to take fire investigation scene photographs when necessary. "Off-Air" communications are communications not on the normal two-way radio system. These devices also serve as an alternative or back-up means of communication in the event of the CREST radio system failure.

2. Scope of this PIA

This PIA reviews Victoria Fire Department's new Sonim Smart mobile phones for compliance with FIPPA's privacy provisions. A second separate PIA will be completed for the Victoria Fire Department's Mobile Data Terminals (MDTs) being implemented in the fall 2015, which have a similar use case to the mobile phones.

3. Related Privacy Impact Assessments

VFD Prevention Tablet PIA

https://worksites.victoria.ca/sites/Teams/TeamTemplate/FireSupport/Team%20Documents/Fire%20Prevention%20Units/PIA%202016%20VFD%20Prevention%20Tablets.docx

VFD Mobile Data Terminal PIA

https://worksites.victoria.ca/sites/Teams/TeamTemplate/FireSupport/Team%20Documents/MDT%20Fire%20Mobile%20Units/PIA%202015%20VFD%20MDT.docx?web=1

4. Elements of Information or Data

Photographs of Incidents: VFD staff will, from time to time, take photographs of incidents for record keeping and to assist with incident report writing. Most of the photographs will not contain

personal information. However, some photos may include:

a. Deceased individuals, vehicle licence plate numbers, onlookers, and personal items such as family photographs.

b. Photos themselves may not identify individuals, but could if matched against information provided by newspapers (e.g. providing the name of a deceased or the bedroom location and name of an individual)

b) Photographs may be shared to other Victoria Fire Department mobile devices via MMS. Photographs are also downloaded off the devices to the Captain's computer (two at HQ, 1 at Hall 2 and 1 at Hall 3) via a USB connection.

c) Photographs of Buildings: VFD staff will sometimes take photographs of particular locations of buildings related to fire incident pre-planning and training purposes. For example, electrical panels, standpipes, gas meter shut off locations, apparatus staging location, stairwells, exit locations, etc.

d) Photographs of Staff: VFD staff may also take photographs of other staff members during an incident (fire, Motor Vehicle Accident (MVA) for example) to assist with record keeping and report writing. Photographs could also be used for education and training purposes.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The mobile devices do not use any storage outside of Canada. Photographs are stored directly to the mobile devices internal memory.

a) Governance:

- Written policy will be/has been developed about how the devices are to be operated and secured by staff. This policy will outline controls for data captured by the devices, how long that data will be stored, and a response plan should the security of the device be breached.
- Staff are instructed to avoid taking photographs of bystanders or innocuous interactions with the public
- Staff are instructed to only send photographs to other VFD mobile devices, not to personal devices.
- Staff are instructed to delete the photographs from the mobile phones once they have been downloaded to the Captain's desktop computer.
- Staff are instructed to never photograph children's faces
- Staff will only collect as much personal information as is needed for a legitimate business purpose

b) Security features for system maintenance, patch updates, synchronization:

- Auto-updates to the mobile phones are disabled; only authorized users (IT and VFD Admin) are permitted to make updates to the OS or mobile apps.
- Updates are reviewed, tested and updated quarterly or as required.

c) Transmission security:

- Photographs may be sent over the Bell mobile network via MMS to another VFD mobile phone. They can be sent to any mobile number, but policy will establish rules restricting sharing to other VFD mobiles.
- Most often, photographs will be manually downloaded off the mobile via USB to a secure City of Victoria desktop computer to preserve the photograph quality.

d) Back-up locations of personal information:

- City of Victoria IT takes backups of its databases daily. These photos will be part of that backup.

6. Data-linking Initiative*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The linkage purpose is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No

7. Common or Integrated Program or Activity*

If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	VFD staff will take photographs on scene, where required or applicable.	collection	26(b), 26(c)
2.	VFD personnel will manually download the photographs from the mobile device. Once complete, the VFD personnel will delete all photographs from the mobile device.	use	32(a)
3.	VFD Captain will attach the photograph to the incident narrative in FDM.	use	32(a)
4.	Photos are used to investigate fires	use	32(a)
5.	Other VFD access the photos	disclosure	33.2(a), 33.2(c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Access to email accounts	There are no user accounts configured to the devices. Users would have to log in to a web-based email service.	low	med
2.	Use of SMS	Staff will receive training on the proper use and distribution of photographs with the mobile devices. Policy will be developed that outlines guidelines for proper use of the mobile phones and SMS.	low	med
3.	Data retention	Records will be maintained as per normal fire record retention periods. Photographs related to incidents will be saved in the FDM database.	low	med
4.	Victim identification	Disclosure of photographs to people who do not have a "need to know".	low	med
5.	Loss of Phones	Access to phones are protected and memory can be remotely wiped	low	med

10. Collection Notice

A collection notice is not required. Personal information is collected indirectly under section 27(1)(b) and 27(3)(c).

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

The six Sonim smart mobile devices are not assigned to specific user. They are attached to an apparatus with four rotating platoons. They do not require user accounts and they are not configured to of have email accounts.

Security of mobile devices:

- All personal information sharing is limited to only VFD staff

Devices are stored in the apparatus when not on an active call. When on a call, the devices will remain in the apparatus until On Scene, then they will be kept either on staff or remain in the apparatus. The apparatus doors are never locked. These mobile devices stay on the apparatus unless required on scene.

12. Please describe the technical security measures related to the initiative (if applicable).

- A four-digit PIN is enabled on the devices. The Deputy Chief of Operations created the PIN and communicated this PIN to all staff authorized to use the mobile devices.
- If a device is stolen, 5 failed login attempts will lock the device.
- The devices mobile device management system (MDM) will be Microsoft InTune. This application allows IT to monitor the physical location of the device, review and control internet search history, and provides the ability to remotely lock and erase the device should it be lost or stolen.
- If a device is lost or stolen, it will be immediately locked by IT.
- If a device is lost and cannot be retrieved immediately, it will be remotely erased by IT.
- The mobile devices will lock after 5 minutes of inactivity. After this period, the four-digit PIN will be required to unlock the device.
- All Suppression staff and the Deputies of Administration and Operations will know the PIN numbers to the mobile devices.

13. Does your branch/department rely on any security policies?

All staff at VFD have been trained in the proper use of the mobile devices. This training includes instruction on privacy awareness and the proper situations to take photographs. It also reviews how photographs will be downloaded and deleted from the devices regularly. During training, the proper use of City assets is reviewed to emphasize not using the mobile devices for non-work related personal information.

Deputy Fire Chiefs, Battalion Chiefs, Captains, Fire Prevention Officers and the Fire Prevention Clerk have access to FDM where the incident records are held.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The mobile devices at VFD have the Apex Launcher installed, which prohibits the ability of users from making changes to their configuration or settings. Users do not have the ability to add any additional mobile apps.

Only IT staff and Specific VFD staff can alter the phones' configuration and/or settings. At Victoria Fire Department, the instruction for accessing the phone's configuration and settings has been shared with the Deputy Chief of Operations, and Deputy Chief of Administration, and the Master Mechanic. At the City of Victoria, Information Technology Division, the City's internal Helpdesk staff have been provided the information to modify the configuration settings. This configuration document has been saved to the City's internal issue tracking system, Footprints, so it can be accessed by IT staff in the event of an emergency and for redundancy. This configuration document was written by IT's Business Solutions Analyst, Katherine Wilson.

Anyone with the ability to unlock the launcher app has the ability to add additional apps to the mobile device. Only administrators can add additional apps to the mobile devices once they have been vetted by Deputy Chief of Operations and tested on a device prior.

15. Please describe how you track who has access to the personal information.

VFD Admin keeps track of all staff on shift for each platoon. Typically, it is the Officer on each apparatus that is the primary user of the mobile phone. As the devices are not attached to any particular user, any staff member at VFD may use the device as required.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

The mobile phone cameras are used only for the purpose of taking incident scene photographs. They will not be altered, but may have narrative describing each photograph if necessary.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

22. Will a personal information bank (PIB) result from this initiative?

No

Part 6 – Privacy Officer Comments

1. Advise the Information Access and Privacy Analyst if any changes to the collection, use and disclosure of the personal information collected by the phones changes.

2. Advise the Information Access and Privacy Analyst if a privacy breach of the personal information on the phones occurs.

3. Create a policy on when a device should be locked and when its information should be erased.

Part 7 – Program Area Signatures

Rob Gordon		May 6/16
Privacy Officer/Privacy Office Representative	Signature	Date
Dan Atkinson		May 3/2016.
Program/Department Manager	Signature	Date
MIKE PALMER		May 2/2016
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Head of Public Body, or designate	Signature	Date