ATTACHMENT A

CITY OF NANAIMO
THE HARBOUR CITY

Information Report

DATE OF MEETING April 08, 2019

AUTHORED BY MEGAN WAGGONER, RECORDS/INFORMATION & PRIVACY COORDINATOR

SUBJECT **OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FINDINGS AND RECOMMENDATIONS**

OVERVIEW

Purpose of Report
To provide Council with an update on the recommendations of the Office of the Information and Privacy Commissioner.

Recommendation
That Council endorse Staff's initiatives to endeavor to comply with all of the recommendations of the Information and Privacy Commissioner of British Columbia.

DISCUSSION

On August 2, 2018, British Columbia's Information and Privacy Commissioner, Michael McEvoy, wrote a letter to the City of Nanaimo advising of the conclusion of the Office of the Information and Privacy Commissioner's (OIPC) investigation into several breaches of personal information (Attachment A). In his letter the Commissioner outlined the following recommendations that the City must comply with:

The Commissioner recommended that:

1. The City take immediate steps to implement a Privacy Management Program. The program should include:

    a. designating a staff member responsible for reviewing the City's privacy policies and security arrangements relating to the protection of personal information in the City's custody or control; and

    b. a privacy policy that applies to every instance of collection, use or disclosure of personal information, as a necessary component of the diligence required by s. 30 of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

2. The City conduct comprehensive mandatory and ongoing privacy training for all employees and officers to ensure those who handle personal information are made aware of their obligations under FIPPA.

The position of Claims/FOI Coordinator, which has the delegated authority of the Freedom of Information (FOI) Head under "Freedom of Information and Protection of Privacy Bylaw 2006 No. 7024" has been updated to reflect the requirements set out in recommendation 1(a), and is now titled Records/Information & Privacy Coordinator. This position, under the direction of the FOI Head, will be responsible for implementing and maintaining a Privacy Management Program for the City, which will include improved records management practices and policies; a new records classification and retention schedule which will identify personal information banks and appropriate records retention and destruction timelines; implementation of a privacy policy that applies to every instance of collection, use, or disclosure of personal information (attached); and various other elements of a functioning Privacy Management Program.

In regards to the second recommendation, the City has increased staff education opportunities significantly since 2017 when the OIPC investigation commenced. Legislative Services staff have attended departmental staff meetings for various departments where staff have given verbal presentations about *FOIPPA*, and provided handouts relevant to the departments such as: OIPC orders; *FOIPPA* handouts; routinely available records list; and, answered staff questions specific to their job functions.

The Legislative Services department has been working with the Human Resources (HR) Department to schedule mandatory training for all staff. Historically there has been voluntary *FOIPPA* training offered once annually to staff who wish to attend, this training has been organized and tracked through the HR Department and taught by the FOI Head. In 2019, we have increased this training to three sessions a year provided through the HR Department, as well as attending other City facilities every two months to provide smaller group training courses. This training will be mandatory for all staff and attendance will be tracked through the HR Department. Where the departmental training courses have typically been fairly informal, we will now take the same course content noted above to these smaller meetings in order to ensure that all required content is covered by all staff. Additionally, there has been a *FOIPPA* component incorporated into the Corporate Orientation, which is provided twice a year to new employees as well as employees who have changed from temporary to permanent employment status. Our hope is that with this rigorous training schedule, we will be able to deliver the appropriate training to staff and increase privacy awareness throughout the City of Nanaimo.

In his letter, the Commissioner notes that those who are entrusted to serve the public and who possess personal information by reason of their public duties have a responsibility to treat it with respect and in compliance with the law. All City of Nanaimo officers and staff must understand and employ the fundamental practices required to protect personal data – from secure methods to collect, store and transmit personal data through to secure methods of destruction. Everyone in the organization has a role to play in protecting the personal information that the organization collects, uses, and discloses, and every individual within the organization contributes to the success of the program.

SUMMARY POINTS

- The Information and Privacy Commissioner of British Columbia has made several recommendations to the City of Nanaimo.
- Staff are taking the necessary steps to meet the recommendations of the OIPC and comply with the *Freedom of Information and Protection of Privacy Act.*
- Staff will require the support of Council and the Senior Leadership Team in order to comply with the recommendations and implement a successful Privacy Management Program.

ATTACHMENTS

OIPC F17-72024 Privacy Breach Investigation – Attachment A
DRAFT City of Nanaimo Privacy Policy – Attachment B

Submitted by:	**Concurrence by:**
Megan Waggoner, Records/Information & Privacy Coordinator	Sheila Gurrie, Corporate Officer and FOI Head

Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency

August 2, 2018

Sheila Gurrie
Corporate Officer
City of Nanaimo
455 Wallace Street
Nanaimo, BC V9R 5J6

Dear Sheila Gurrie:

Re: Privacy Breach Investigation – OIPC File F17-72024

I write regarding reports you made to my office on behalf of the City of Nanaimo about three separate personal information disclosures.[1] You reported that the information in question was in the City's custody and control and was disclosed without any legal authority.

When an unauthorized disclosure of personal information is reported to the OIPC, my staff, expertly versed in such matters, normally help the public body or organization manage it. In the normal course of business, this means giving advice about preventing further disclosures and helping determine whether individuals affected by a disclosure should be notified. Usually, the public body or organization and its leadership are responsible for remedying a privacy breach, with oversight from the OIPC.

However, in this case, the disclosure reports to my office implicated senior members of the City's leadership, thereby casting doubt on the City's ability to properly remedy the alleged breaches. The former acting commissioner consolidated all of the matters you reported to our office into one investigation under s. 42(1)(a) of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

On November 2, 2017, the former acting commissioner advised the City of the purpose of the investigation – to examine and assess the cause and extent of these disclosures and to assess the measures the City has taken to protect personal information and comply with the security measures required by FIPPA.

I have decided to post this reporting letter on our website given that the issues addressed in this review have been the subject of considerable public discussion and debate in Nanaimo. This letter also serves to remind those who serve in municipal offices that the public has entrusted them to protect the personal information within their custody or control and that they must take all reasonable measures necessary to do so.

[1] You are a designated "Head" of the City under s. 77 under FIPPA.

Background

My staff interviewed a number of City employees and councillors under oath about the information disclosures as well as the privacy management practices at the City. Investigators collected and examined records relating to the incidents as well as information about the City's privacy management program.

My investigators observed significant adversarial relationships between some members of the council and administration. Those relationships are not within my authority to investigate. I mention them here only because it provides some context for the findings that follow.

The information at issue in the three disclosures is summarized as follows:

1. The workplace report

The City's Chief Administrative Officer (CAO)[2] complained to the City's Human Resources department in early 2017 that certain conduct toward her violated the City's "Respectful Workplace Policy". In response, the department retained an outside consultant to determine whether the policy was breached.

The consultant provided a workplace report to the Director of the City's Human Resources department on July 20, 2017. The report contains sensitive personal information about the complainant and several other individuals. In general terms, the report concerns allegations of conflict and dysfunction between some members of City council and City administration.

2. The consulting group email

On March 31, 2015, the City's mayor wrote an email to a consulting group and copied the City's then CAO. The purpose of the email was to engage the firm to assist in resolving adversarial relationships on council. Among other things, the email contained the Mayor's opinions about City councillor colleagues, some of which were not complimentary.

3. The two law firm letters

Two letters were sent to the City from a law firm representing a City Councillor:

- a letter dated December 10, 2015 addressed to the City's mayor; and
- a letter dated December 14, 2015 addressed to the City's Chief Administrative Officer (CAO).

[2] The CAO has since left the employ of the City.

The letters set out concerns about how certain City personnel matters were handled by council. The letters name several individuals in relation to those concerns.

Application of FIPPA

Personal information can only be disclosed with legal authority

The City of Nanaimo, like all public bodies in BC, is subject to FIPPA. The requirements of the legislation extend to all of the City's officers and employees, including the Chief Administrative Officer, the mayor, and councillors. Part 3 of FIPPA sets out specific rules about how personal information in the City's custody or control must be treated.

FIPPA defines "personal information" as information about an identifiable individual. This definition has been interpreted in court decisions to mean any information that is capable of being linked to an identifiable individual, on its own or in connection with other available information.

Section 30.4 of FIPPA prohibits the disclosure of personal information by City employees, officers and directors except as authorized by FIPPA.

Obligation to protect personal information

Under s. 30 of FIPPA, public bodies, such as a city government, must make "reasonable security arrangements" to protect personal information in their custody or control from unauthorized access or disclosure. What constitutes reasonable security arrangements is contextual and can vary according to factors such as the sensitivity and amount of the personal information. Orders by my office note that while "reasonable" does not mean perfect, it does signify a very high level of rigour.

Application of FIPPA to the disclosures in this case

As the City's head under FIPPA, you reported to my office that the workplace report, the consulting group email and the law firm letters were within the City's custody and control; contained personal information; and that this personal information was disclosed without authority. In short, these were privacy breaches.

On review, my investigators confirmed the report, email and letters were within the City's custody or under its control and that they contained personal information. The question therefore is whether the report, email and letters containing the personal information were disclosed and if so did this happen without legal authority provided under FIPPA. I consider each matter in turn.

Workplace report

The consultants delivered the report to the City's Human Resources department on July 20, 2017. The department then provided a copy to the CAO and two individuals named in it. The Human Resources department temporarily[3] stored the report on a shared computer drive accessible to department staff.

Copies of the report were also circulated to city councillors at a July 26, 2017 in-camera council meeting. Those councillor copies were collected and returned to the Human Resources department at the end of the in-camera meeting.

On August 2, 2017, a major newspaper published an article stating that it was provided with a copy of the report. The article's author noted that the report had not been publicly released. There is no reason to doubt the newspaper's story that it was given a copy of the report. I therefore find the report, within the City's custody and control, was disclosed to the newspaper and there was, on its face, no legal authority for doing so.

We asked the CAO if she disclosed the report as she was quoted in the newspaper article saying she was afraid the report would not be made public. The CAO admitted to making that statement but denied disclosing the report to the newspaper. We also asked the other interviewees if any of them had disclosed the report. All denied doing so.

My investigators reviewed all other relevant evidence that they had collected in addition to the testimony taken under oath. Having carefully assessed it, my staff were unable to conclusively establish who disclosed the report to the newspaper.

While I find that the disclosure of the personal information in the report was not authorized by FIPPA, there was insufficient evidence to determine who at the City contravened s. 30.4 of FIPPA.

Consulting group email

A copy of the Mayor's email to the consulting group was described, but not provided, by the CAO at an in-camera meeting of City council on or about March 21, 2016. On April 4, 2016, council passed a resolution requiring the CAO to provide it with a copy of the email. The CAO provided council with a copy of the email on June 22, 2016 redacting much, but not all, of the personal information of councillors.

A member of the public presented an unredacted copy of the email to an open meeting of City council on November 21, 2016. He said he found the email on his car windshield.

I find that the disclosure of the personal information in the email was not authorized by FIPPA, but my staff could not conclusively determine who provided the email to the

[3] Less than five days.

member of the public. The likely source of the email was from within the City, considering that the consulting group had little to gain from its disclosure. We interviewed City employees and officials who we identified as having had contact with the email. However, they all denied disclosing it, and we found no other independent evidence that conclusively demonstrated who released it.

Two law firm letters

City staff distributed the December 10, 2015 letter to the Mayor from a law firm for discussion at a December 16, 2015 in-camera meeting of City council. The City could not confirm whether the December 14, 2015 letter was also distributed for the same meeting.

One councillor stated under oath to my investigators that he had received both letters by email for the purposes of an in-camera council meeting. He said that neither the email attaching the letters nor the letters themselves explicitly stated that they were confidential. He said that he disclosed both the December 10, 2015 and December 14, 2015 letters by posting them on a Facebook page that he administers.

On May 25, 2016, the City issued a written notice, pursuant to s. 73.1 of FIPPA, to the councillor demanding that he remove the information from this Facebook page. In response the councillor removed the information.

As described above, City councillors are officers of the City. They may only disclose personal information in the City's custody or under its control if there is authorization under FIPPA to do so. As the City's head, you are responsible for dealing with privacy breaches. You submitted there was no authority to disclose the personal information in the letters and I agree. The councillor in question is an experienced member of council and knew that documents distributed in-camera were not to be disclosed beyond council chambers. Common sense dictated that the lack of a "confidential" label could not be interpreted as a green light to release personal information in contravention of FIPPA, particularly given that the meeting was in-camera.

I find that the disclosure of any personal information in the letters by the councillor on the Facebook page was not authorized by FIPPA. While this constituted a contravention of s. 30.4 of FIPPA, the councillor properly took down the letters that he posted when the City first demanded that he do so under s. 73.1.

Consulting group email and December 14, 2015 law firm letter remain posted

During this investigation my staff discovered that, in addition to the councillor posting the December 14, 2015 law firm letter on the Facebook page he administers, a member of the public also posted it to this page on May 19, 2016. When clicked, the hyperlink disclosed the December 14, 2015 law firm letter. We also learned that the same member of the public posted the consulting group email on the Facebook page on

November 22, 2016. The councillor administers and is responsible for that Facebook page and therefore controls its content.

The City issued written notices to the member of the public referred to in the preceding paragraphs, pursuant to s. 73.1 of FIPPA, on May 24, 2016 and on November 22, 2016 respectively, given that he possessed both the law firm letters and the consulting group email.

On May 27, 2016, the member of the public advised the City that he had destroyed the law firm letters. However, on November 27, 2016, in respect of the consulting group email, the member of the public stated that he would not destroy it.

We have discussed the November 27, 2016 response the City received from the member of the public. The City has now advised my office that it will re-issue a written notice, pursuant to s. 73.1 of FIPPA to the member of the public.

The City also advised my office that on July 25, 2018, it issued a further s. 73.1 notice to the councillor requiring him to securely destroy the documents posted on the Facebook page by the member of the public.

If the councillor refuses the City's demands, the City can ask the Attorney General of BC to petition the Supreme Court of British Columbia to enforce them. The City advises my office that it intends to do so if the councillor does not comply. I support the City's planned course of action and my office will assist the City as appropriate.

The posts containing personal information that appear on the Facebook page administered by the councillor, as of the writing of this letter, also constitute a contravention of s. 30.4 of FIPPA and can be prosecuted pursuant to s. 74.1. Prosecution of an offence under FIPPA by my office remains an option pending the outcome of the City's actions.

Protecting Personal Information

This letter should not be taken as criticism of the actions you have taken as the City's Corporate Officer and head under FIPPA. During our investigation, you, along with other City staff, cooperated fully with my investigators and took steps, as best you could, to protect personal information within the City's custody or control. Indeed, you reported the disclosures to my office and acted to contain the breaches by ordering the recovery of the improperly disclosed personal information. I commend you for this. The steps you took are those I would expect a public body to take when managing a privacy breach.

Nevertheless, our investigation found that the disclosures of the personal information in the report, email and letters were not authorized by FIPPA. In reviewing the evidence, I can see that some officers of the City, including some members of council, lack a basic understanding of their privacy obligations under FIPPA. The City needs to remedy this to prevent future abuse.

I recommend that the City take immediate steps to implement a privacy management program to ensure it can meet all of its obligations under FIPPA. Executive-level support is the backbone of successful privacy management. City council and officers of the City should lead by example by demonstrating commitment and support for effective privacy management.

This program should include designating a staff member responsible for reviewing privacy policies and security arrangements in place to protect the personal information in the custody or under the control of the City. A privacy policy that applies to every instance of collection, use or disclosure of personal information is a necessary component of the diligence required by s. 30.

I further recommend that all employees and officers of the City who handle personal information be made aware of their obligations under FIPPA. This privacy training should be comprehensive, mandatory and ongoing for all employees and officers. The City should track participation in that training.

Conclusion

Those who are entrusted to serve the public and who possess personal information by reason of their public duties have a responsibility to treat it with respect and in compliance with the law.

While there may be, in extraordinary circumstances, a lawful basis for public disclosure of sensitive personal information in a public body's custody or control, this is clearly not one of them. In this case, personal information was disclosed contrary to law and to the duty of trust required of public officials.

I have directed a senior member of my office to meet with members of council and senior City staff to discuss their legal responsibilities as outlined in this letter. I trust that the remedial approach I am taking in this case will ensure that I do not see a repeat of such incidents in Nanaimo.

My staff will follow-up with you for an update on the City's implementation of the recommendations in this reporting letter by November 20, 2018.

Sincerely,

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

ATTACHMENT B

CITY OF NANAIMO
THE HARBOUR CITY

COUNCIL POLICY

Section:	**Administration**	**1**
Subsection:	**Information and Privacy**	**0580**
Title:	**Privacy Policy**	**01**

REASON FOR POLICY

The purpose of the City of Nanaimo's Privacy Policy is to describe how the City collects, uses, discloses and protects personal information. This policy provides a framework for how the City will operate in order to ensure personal information is managed in accordance with the *Freedom of Information and Protection of Privacy Act.* This policy also gives examples of what personal information the City needs, and examples of how it uses and discloses personal information.

SCOPE

This policy applies to personal information that the City collects, uses or discloses in any form (including verbal, electronic or written personal information).

This policy does not apply to any collection, use or disclosure of personal information through the City's website. The City's website privacy policy can be accessed through this link: https://www.nanaimo.ca/privacy-policy

DEFINITIONS

The following definitions are used in this policy:

a. "Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia);

b. "City" means the City of Nanaimo;

c. "employee" means an employee of the City, including a volunteer;

d. "personal information" means recorded information about an identifiable individual;

e. "service provider" means a person we retain under a contract to perform services for us;

f. "us" refers to the City, as do "our", "we" and similar terms, not to any employees or elected or appointed City officials;

g. "you" refers to anyone whose personal information we collect, use or disclose

POLICY STATEMENT

This policy is established in accordance with the City's *Freedom of Information and Protection of Privacy Act Bylaw 7024.* We protect the personal information we collect, use and disclose in accordance with the *Freedom of Information and Protection of Privacy Act* (*FIPPA)* by promoting privacy awareness, applying sound privacy principles and implementing reasonable security measures.
This policy is the foundation for the City's privacy management program. It sets the framework for privacy to be a central component of our business practices and a built-in component of our day-to-day program operations.

POLICY

1. COLLECTION OF PERSONAL INFORMATION

We collect personal information:

a. where collection is authorized under a statute, which may include the *Community Charter,* or is authorized under City bylaws;

b. for the purposes of our activities, services and programs;

c. for the purposes of planning or evaluating our activities, services and programs;

d. for law enforcement purposes, including enforcing our bylaws; and

e. at presentations, ceremonies, performances, sports meets, or similar events, that are open to the public and where you voluntarily appear.

We collect your personal information directly from you, but we may also collect it from another source if you have consented to our doing so. We may collect your personal information from another source in these cases:

f. where another law allows us to do so;

g. for law enforcement, for a court proceeding, to collect a debt or fine from you, or to make a payment to you;

h. where your personal information is necessary for us to deliver, or evaluate, a common or integrated program or activity;

i. where your personal information is necessary to establish, manage or terminate an employment relationship between you and us;

j. if your personal information may be disclosed to the City under Part 3 of the Act; or

k. where we collect your personal information for the purpose of determining your suitability for an honour or award.

2. CONSENT, USE AND DISCLOSURE OF PERSONAL INFORMATION

We will use and disclose your personal information only for the purpose we collected it for or for a purpose that is consistent with why we collected it in the first place. We may also use or

disclose your personal information for another purpose if you have identified the information and consented to our other use. Lastly, we may use your personal information for a purpose for which it can be disclosed to us under Part 3 of the Act.

We may also disclose your personal information:

a. if you have identified the information and consented in writing to its disclosure;

b. to our employees or service providers if the information is necessary for their duties, for delivery of a common or integrated program or activity, or for planning or evaluating a City program or activity;

c. if your personal information is made publicly available in British Columbia by a law that authorizes or requires it to be made public;

d. to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;

e. to your union representative who is making an inquiry, if you have given the representative written authority to make the inquiry or it is otherwise authorized;

f. to our legal counsel for the purpose of legal advice or for use in legal proceedings involving us;

g. to your Member of the Legislative Assembly if you have asked her or him to help resolve a problem; or

h. as otherwise permitted under Part 3 of the Act.

Please note that all information provided at open meetings of Council or its committees is considered to be public. If you provide or disclose your personal information to us for that purpose, you are consenting to that information being available to the public, including through posting on our website. This information is considered to be a part of the public record and cannot be removed or changed. However, if you satisfy us in advance that you have legitimate personal safety concerns for yourself or an immediate family member, we may allow you to submit your personal information to Council or a committee in confidence. We will not make it publicly available in that case, although we will keep it in our Legislative Services office, as part of the record.

Express consent is always required when personal information is considered sensitive. Consent can be obtained in a variety of ways, including but not limited to: in person, by mail, by phone, and via the internet. Consent clauses should be easy to find and use clear and straightforward language. Records are to be kept of the consent received such as by notes to file, copy of email, copy of check-off boxes, and signature next to statement on forms. If you wish to withdraw consent at any time, please contact the Legislative Services department.

3. ACCURACY OF PERSONAL INFORMATION

We make every reasonable effort to ensure that personal information we use to make a decision directly affecting you is accurate and complete.

4. ACCESS TO PERSONAL INFORMATION

You can ask us to give you a copy of your personal information that is in our custody or control by contacting the Legislative Services department. If you are an employee and would like a copy of your own employee personal information, you will need to contact the Human Resources department.

If we believe your request may involve someone else's personal information, or information protected under the Act, we may require you to make a formal request under the Act for access to records. The Act gives us 30 business days to respond to a formal request, starting on the date your request is received (the Act also allows that time to be extended). Please note that in some cases the Act may require us to refuse you access to even your own personal information. We will give you written reasons for every decision on a formal request.

Before disclosing your personal information, we will require you to verify your identity, so we can be assured that you are the individual whose information is being requested. This helps ensure we do not disclose your personal information to someone we should not give it to.

5. CORRECTION OF PERSONAL INFORMATION

If you believe there is an error or omission in your personal information that we have, you can contact us in writing and ask us to correct it. If we are satisfied that your request is reasonable, we will correct your information as soon as reasonably possible. If we decide not to correct your information, we will note your requested change on the information as well as why we did not correct your information as you asked. This paragraph applies only to factual errors or omissions of your personal information that is in our custody, not opinions or evaluations about you.

6. RETENTION AND DISPOSAL OF PERSONAL INFORMATION

If we use your personal information to make a decision that directly affects you, we will keep it for at least one year after we make our decision. We also keep personal information in accordance with our relevant record retention schedules. We use reasonable efforts to ensure that your personal information is destroyed securely when the time comes under our records retention schedules.

7. RESPONSIBLE USE OF INFORMATION AND INFORMATION TECHNOLOGY

Your privacy matters to us, so we use what we believe are reasonable security arrangements to protect your personal information against such risks as unauthorized access, collection, use and disclosure. These arrangements may include information technology measures, as well as policies and practices, to protect your personal information.

If we disclose your personal information to our service provider, we will make reasonable efforts to impose contractual protections on the service provider. Those protections vary according to the nature and sensitivity of the personal information involved. We require our service providers not to use or disclose personal information other than for the purpose of performing services for us.

All employees are required to respect the confidentiality of personal information they receive or compile and are required to use and disclose it only in accordance with this policy and the Act.

8. RESPONDING TO PRIVACY-RELATED COMPLAINTS

Any complaint about any privacy-related matter under this policy or under the Act must be made to us in writing.

We will consider your complaint, including about a breach of your privacy, and will disclose the outcome to you in writing. We expect you to co-operate reasonably and in a timely way with our work, including by promptly providing us with information that we might reasonably need to do our work.

You can seek advice or information from the Office of the Information and Privacy Commissioner for British Columbia. You can also make a written formal complaint to that Office, although we encourage you to use our complaint procedure first. Wherever we can, we try to work things out directly with people, to their satisfaction.

9. EDUCATION AND AWARENESS

All City employees require training on *FIPPA* and privacy generally as appropriate to their work function. Additional training is required in the following circumstances:

- Employees handling high-risk or sensitive personal information electronically require training related to information systems and their security, in co-ordination with the IT department's training.
- Employees managing programs or activities require training related to privacy impact assessments.
- Employees managing common or integrated programs or activities require training related to information sharing agreements.

10. PRIVACY RISK ASSESSMENT

Privacy impact assessments (PIAs) are conducted to determine if a current or proposed system, project, program or activity meets or will meet the requirements of Part 3 of FIPPA. A PIA will be done for all new projects involving personal information and for any new collection, use or disclosure of personal information. It will also be conducted for common or integrated programs or activities and data-linking initiatives as well as when significant modifications are made to existing systems, programs or activities.

11. PRIVACY BREACH MANAGEMENT & PROTOCOLS

Information regarding our procedure for responding to a privacy breach is outlined in the document RM-05 Privacy and Information Security policy.

12. SERVICE PROVIDER MANAGEMENT

Employees who prepare or manage contracts are to include the privacy protection schedule or standard privacy language, as designated by the Privacy Officer, in all contracts that involve the service provider having access to, or collecting, using or disclosing, personal information in the custody or under the control of the City.

13. EXTERNAL COMMUNICATIONS

We will contact an individual in the following circumstances:

- To give notice of collection of their personal information
- When individuals request access to their personal information or access to records where someone else's personal information is involved
- When responding to requests for correction of personal information
- When personal information is disclosed without consent for compelling health or safety reasons
- When the City intends to give access to personal information in response to a freedom of information request.

14. ROLES & RESPONSIBILITIES

Chief Administrative Officer

- Approves policy and procedures and ensures all employees are given notice of, and access to, a copy of the policy.

Department Heads

- Support and co-operate with the Privacy Coordinator in implementing the policy and in complying with *FIPPA*.

Corporate Officer/FOI Head

- Responsible for overseeing the duties and responsibilities of the Records/Information & Privacy Coordinator

Records/Information & Privacy Coordinator

- Under the direction of the FOI Head, responsible for the development, management and implementation of the City's privacy management program including ongoing assessments and revisions.
- Coordinates employee training and education, ensuring that all new employees receive *FIPPA* orientation and training within the first year of their employment.

See RM-02 Records Management Accountability Policy for full listing of roles and responsibilities with respect to management and governance of information and records.

CONTACT INFORMATION

If you have any questions about this policy or your personal information please contact Legislative Services at (250) 755-4405 or by email at foi@nanaimo.ca

AUTHORITY TO ACT

The Corporate Officer is delegated responsibility and authority for ensuring compliance with this policy and *FIPPA*.

RELATED DOCUMENTATION

Legislation
City of Nanaimo's Freedom of Information and Protection of Privacy Bylaw 2006 No. 7024
Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165)

Records Management Policies and Procedures
RM-01 Records Management Framework Policy
RM-02 Records Management Accountability Policy
RM-03 Records Management Policy
RM-04 Legal Hold Policy
RM-06 Scanning and Imaging Policy
RM-07 Email Management Policy
RM-08 Vital Records and Business Continuity Policy
RM-09 Access to Information Policy
RM-10 Mobile Device Policy
RM-11 Records in the Custody of Council Policy

POLICY REVIEW

This policy shall be reviewed by the Corporate Records Officer at least every 3 years.

Date: 201X-XXX-XX Approved by: