ANNUAL REPORT 2017/2018

NUNAVUT INFORMATION AND PRIVACY COMMISSIONER

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF NUNAVUT

P.O. Box 382
Yellowknife, NT
X1A 2N3

July 27, 2018

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: Hon. Joe Enook
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit to the Legislative Assembly my Annual Report as the Information and Privacy Commissioner of Nunavut for the period of April 1st, 2017 to March 31st, 2018.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

In Yellowknife: 867-669-0976 ○ Toll Free: 888-521-7088 ○ Fax: 867-920-2511 ○ Email: admin@atipp-nu.ca

CONTENTS

COMMISSIONER'S MESSAGE _____ 7
ACCESS TO INFORMATION AND PROTECTION OF PRIVACY IN BRIEF _ 13

Access to Information 13
Protection of Privacy 14
The Role of the Information and Privacy Commissioner 15

THE YEAR IN REVIEW _____ 17
REVIEW REPORTS ISSUED _____ 20

Review Report 17-116 20
Review Report 17-117 21
Review Report 17-118 22
Review Report 17-119 24
Review Report 17-120 25
Review Report 17-121 26
Review Report 17-122 27
Review Report 17-123 28
Review Report 17-124 29
Review Report 17-125 30
Review Report 17-126 31
Review Report 17-127 32
Review Report 17-128 33
Review Report 17-129 33
Review Report 17-130 34
Review Report 17-131 35
Review Report 17-132 37
Review Report 17-133 38
Review Report 17-134 40
Review Report 17-135 41
Review Report 18-136 42
Review Report 18-137 44

Review Report 18-138 45
Review Report 18-139 46
Review Report 18-140 47
Review Report 18-141 48
Review Report 18-142 49

TRENDS AND ISSUES – MOVING FORWARD _____ 50

Review of Policies..... 51
Focus on File Management 52
Adequate Resources 53
Education..... 54

COMMISSIONER'S MESSAGE

I was appointed as the first Information and Privacy Commissioner of Nunavut in 2000, shortly after division and I have had the honour of serving the people of Nunavut for the last 18 years and before that, as Information and Privacy Commissioner of the Northwest Territories from 1997 until division. The work has changed considerably over the years and, in my opinion, the oversight provided by my office is more important today than it has ever been. The world's political climate has changed and having open and accountable government is, more than ever, vital to maintain our democratic ideals. Layer onto this the fact that information in the world of big data and artificial intelligence is a valuable and sought-after commodity, and the role of the Information and Privacy Commissioner becomes a pivotal check and balance between a government and its citizens.

In the past, I have worked well with the public bodies of Nunavut. This is not to say that we haven't had our differences or disagreements with respect to the application of the law. Nunavut public bodies have, however, always respected the law and by far the majority of my recommendations have been accepted over the years. This is one of the reasons that I have maintained that my office does not require order-making power to ensure that the spirit and intention of the Act are maintained. Over the last year, however, I have become concerned that this may be changing. For example, of the 26 Review Reports issued by my office in 2017/2018, the head of the public body failed to respond within 30 days as required by the Act on 19 occasions. Some remain without a response for months – currently we are very close to eight months since the report was issued in one case and nearly six months for another. In addition to these two, as of the date of the writing of this report there are three more that are all more than three months past due. For those reports for which I did receive a response, in only 5 of 21 responses were my recommendations accepted in full. There have also been problems with delays and failures in responding to Applicants and to the Office of the Information and Privacy Commissioner (OIPC), to the point that in several of my reviews, the public body's

handling of the request was so bad that it was necessary for me to make recommendations to the public body about training and adequate resources for those in the department responsible for responding to ATIPP requests. In several cases, applicants complained because the public body had not responded to their request for information in a timely manner or that public bodies had taken extensions of time to respond that were neither reasonable nor in accordance with the Act. For the first time since the Act came into effect in Nunavut, an Applicant is challenging a public body for its decision not to follow recommendations made by this office in the Nunavut Court of Justice. In short, this year saw a marked decline in terms of compliance with the requirements of the Act by public bodies and a similarly marked decline in terms of responding to, acknowledgment of and respect for the recommendations made by this office. I am troubled by this development and residents of Nunavut should be equally concerned. In *Dagg v. Canada (Minister of Finance)* [1997] 2 SCR 403, Justice LaForest of the Supreme Court of Canada set out the principles inherent in Canada's access and privacy laws. This case continues to define the significance of such laws:

> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry. (para 61)

With respect to the nature of the right to privacy, Justice LaForest wrote:

> The protection of privacy is a fundamental value in modern, democratic states; see Alan F. Westin, Privacy and Freedom (1970), at pp. 349-50. An expression of an individual's unique personality or personhood, privacy is grounded on physical and moral autonomy — the freedom to engage in one's own thoughts, actions and decisions...Privacy is also recognized in Canada as worthy of constitutional protection, at least in so far as it is encompassed by the right to be free from unreasonable

> searches and seizures under s. 8 of the Canadian Charter of Rights and Freedoms.

The Supreme Court of Canada has found that access and privacy statues are "quasi-constitutional" in nature. In *Lavigne v Canada (Office of the Commissioner of Official Languages),* [2002] 2 SCR 773 at para 25, Justice Gonthier addressed this:

> The Official Languages Act and the Privacy Act are closely linked to the values and rights set out in the Constitution, and this explains the quasi-constitutional status that this Court has recognized them as having.

In June of 2017 I submitted to the Standing Committee on Public Accounts, Independent Officers and Other Entities (now the Standing Committee on Oversight of Government Operations and Public Accounts) a comprehensive review of the Access to Information and Protection of Privacy Act, outlining my recommendations for amendments to the Act. This report was prepared at a request of the Standing Committee in their Report on the Review of my 2014-2015 Annual Report. It was my hope that the recommendations contained in this report would lead to a comprehensive (and preferably, independent) review of the Act resulting in a modernized piece of legislation. That has not come to pass at this point and there is no indication that a wholesale review of the Act is in the legislative plan. I renew my recommendation that a full review of the legislation take place as soon as possible, and that this review consider creating a piece of legislation that is more robust and with real consequences for failure to comply with the Act

Amendments to the Act were passed late in 2017, some of which did reflect some of the changes I have been recommending for some years. The Amendments were, however, piecemeal and, in some respects confusing and unnecessary, in particular with respect to the provisions dealing with records subject to solicitor/client privilege. On the positive side, the amendments did set the stage for inclusion of municipalities under the *Access to Information and Protection of Privacy Act*, something I have been advocating for since my first Annual Report more than 20 years ago.

Also on a more positive note, I was thrilled to host Canada's Information and Privacy Commissioners in Iqaluit for our annual meeting in October, 2017. I would like to acknowledge the assistance of the staff of the Legislative Assembly and of my Assistant, Lee Phypers, for their help with logistics and planning. This was a significant undertaking which I could not have pulled off without the willing hands of others to assist.

Canada's Information and Privacy Commissioners and Deputy Commissioners in Iqaluit

Mother nature, for her part, gave us some beautiful fall weather and my counterparts were all extremely impressed with what the City had to offer. Our agenda was packed and included information about advancements in cloud services and blockchain

technology, self-governing First Nations and ATIPP legislation, government data integration/matching initiatives and developments in international law and practice in terms of both access to information and protection of privacy (including the European GDPR). One of the most interesting discussions, for me, was about the e-Quality Project, a partnership of scholars, research and policy institutes, policymakers, educators, community organizations and youth led by Professors Valerie Steeves and Jane Bailey at the University of Ottawa. The project focuses on corporate policies in the digital economy, especially insofar as they concern privacy and ways to promote healthy relationships and respect for equality on-line and is aimed at young people and how they interact with the on-line world.

> The economic model behind e-commerce (i.e. disclosure of information in exchange for service) creates a bias in favour of disclosure. Youth are the key to understanding the privacy implications of this bias, because, as early adopters of online media, they drop terabytes of data (often unknowingly) as they go about their daily lives. This data is processed to target them with behavioural marketing to shape their attitudes and behaviours, often outside the reach of existing regulations because privacy policies do not provide full disclosure of the analytics used (making informed consent difficult), and profiling draws in non-personal data (which sidesteps the consent process).

We were fortunate to have both Professor Steeves and Professor Bailey join our meeting to discuss some of their findings and to share their insight on how youth, in the day of Facebook, Snapchat and Instagram, manage their privacy. It was fascinating to hear about how young people view their privacy and alter their behaviour to protect what they consider to be their most private of information. There is, however, much work to be done to educate our young people on how best to ensure their privacy in the on-line world.

This year also saw the launch of our new website at www.atipp-nu.ca. The website contains a lot of information about the work we do, including all of our Annual Reports and Review Reports, a copy of the Act and Regulations, links to helpful sites from other jurisdictions and organizations and much more information. I would like to acknowledge the photographer, Hank Moorlag, the former Information and Privacy Commissioner for the Yukon for allowing me to use some of his pictures, taken in and around Iqaluit, to help make the site more beautiful.

I am also pleased to acknowledge that my budget has been increased to reflect the addition of a full time Deputy-Commissioner, to be shared with the Northwest Territories office. I am excited to have the extra help, particularly in light of the continuously increasing work-load in recent years. I am currently working on filling that position within the next few months.

In closing, I would like, once again, to acknowledge and thank my assistant, Lee Phypers, for her continued support and assistance. Her dedication, hard work and cheery disposition make my job so much easier.

> The digital age is upon us and our laws are quite simply no longer up to the task. Significant improvements are required to bring our access and privacy rights into the 21st century.
>
> Excerpt from "Accountability for the Digital Age: Modernizing Nova Scotia's Access and Privacy Laws" June 2017

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY IN BRIEF

The *Access to Information and Protection of Privacy Act* (ATIPPA) enshrines two principles:

1. public records must be accessible to the public; and
2. personal information must be protected by public bodies.

It outlines the rules by which the public can obtain access to public records and establishes rules about the collection, use and disclosure of personal information collected and maintained by Nunavut public bodies. It applies to 43 departments, crown corporations, local housing organizations and other agencies in Nunavut.

Access to Information

Part I of the legislation provides the public with the right to request and receive public records and a process for obtaining such records. This right of access is so important to the maintenance of open and accountable government that access to information laws have been deemed to be quasi-constitutional in nature. When the public can see how government is functioning and how they are doing their work, they are better able to participate in government and to hold government and governmental agencies to account. The right of access to government records is not, however, absolute. There must be some exceptions and these limited and specific exceptions are set out in the legislation. Most of the exceptions function to protect individual privacy rights and proprietary business information of the companies which do business with the Government of Nunavut. The exceptions also function so as to allow Ministers and their staff to have free and open discussions as they develop policies and deal with issues.

Requests for Information must be in writing and delivered to the public body from which the information is sought. When a Request for Information is received, the public body must first identify all of the records which respond to the request, then assess each record and determine what portion of that record should be disclosed and what might be subject to either a discretionary or a mandatory exception. This is a balancing act which is sometimes difficult to achieve. The response must be provided to the Applicant within 30 days.

When an Applicant is not satisfied with the response provided by the public body, he/she can apply to the Information and Privacy Commissioner to review the response given.

Protection of Privacy

Part II of the Act provides rules for when and how public bodies can collect personal information, what they can use such information for once it has been collected and in what circumstances that information can be disclosed to another public body or the general public. It requires that all government agencies maintain adequate security for the personal information they hold and that personal information be made available only to those who need it to do their jobs.

This part of the Act also gives individuals the right to ask for personal information held by a public body to be corrected.

In addition, if a public body knows or has reason to believe that there has been a material breach of privacy with respect to personal information under its control, the public body must report that breach of privacy to the individual whose information has been wrongfully disclosed and to the Information and Privacy Commissioner.

The Role of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner (OIPC) was established under the *Access to Information and Protection of Privacy Act* of the Northwest Territories in 1997, prior to division. This legislation was continued in Nunavut on Division Day in 1999. The Information and Privacy Commissioner (IPC) is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly and holds that appointment for a five-year renewable term. This role is currently held by Elaine Keenan Bengts, whose term expires in May, 2020.

The role of the Information and Privacy Commissioner (IPC) is to provide independent oversight over public bodies as they apply the *Access to Information and Protection of Privacy Act*. The independence of the role is vital to the work of the IPC as it allows her to openly criticize government, when necessary, without fear of being removed from office.

When someone has asked for information from a public body and is not satisfied with the response received, they may request a review by the Information and Privacy Commissioner. The IPC is able to review all responsive records and, based on the input of both the Applicant and the public body, will prepare a report and make recommendations. The Information and Privacy Commissioner does not have any power to compel public bodies to either disclose or protect information from disclosure but she is required to provide the Minister of a department or the CEO of a public corporation with recommendations. The Minister or CEO must decide to either accept the recommendations made or to take such other steps as they deem appropriate, within 30 days. The Applicant has the right to appeal the Minister's or CEO's decision to the Nunavut Court of Justice if there continues to be a dispute as to the proper application of the Act to the records in question.

The Information and Privacy Commissioner is also authorized to investigate privacy complaints, including complaints about the failure or refusal of a public body to make a

correction to an individual's personal information. Any person may file a complaint about a privacy issue with the Information and Privacy Commissioner. The IPC will investigate and prepare a report and make recommendations for the Minister or CEO.

The Information and Privacy Commissioner is authorized to initiate an investigation of a privacy issue of her own accord when information comes to her attention which suggests that a breach of privacy may have occurred.

As in the case of an Access to Information review, the Minister or CEO of the public agency involved must respond to the recommendations made by the Information and Privacy Commissioner in privacy breach matters. In these cases, however, the Minister or CEO has 90 days to respond, and there is no right of appeal from the decision made.

Nunavut's Legislative Assembly all Dressed Up to Welcome Canada's Information and Privacy Commissioners - October, 2017

THE YEAR IN REVIEW

The Office of the Information and Privacy Commissioner opened a total of 35 files in 2017/2018, a slight decrease from 2016/2017. Most of the files were quite challenging and involved larger numbers of pages. This follows the general trend across the country where every jurisdiction has seen increasing use of the Act and an ever- increasing number of privacy breach complaints. These factors all put pressure, not only on this office but also on public bodies to meet the legal obligations imposed in the Act. While I have criticized public bodies for failing to meet their responsibilities under the Act, my office has also failed to meet the 180-day time frame for completing a review and preparing reports more than once in 2017/2018. This is solely because the office includes only the Information and Privacy Commissioner, and the time of the IPC is shared with the Northwest Territories. It is simply no longer possible to keep up with the volume of work coming into the office with only one person doing the work for two separate jurisdictions. It is hoped that with the addition of a full time Deputy Commissioner (also to be shared with the Northwest Territories) in the next few months, will address this problem. More resources, however, are needed within public bodies and ATIPP Coordinators within the public bodies must be given the time necessary to meet their responsibilities under the Act, particularly in those departments which receive a lot of requests for information or deal with sensitive personal information. Both Finance and Health should have full time, dedicated ATIPP Coordinators whose job responsibilities include actively monitoring privacy policy compliance as well as responding to ATIPP requests.

During fiscal 2017/2018, files opened by the OIPC included consideration of several categories of issues:

Access to Information Matters	
General Requests for Review	21
Adequacy of the Search for Responsive Records	10

Fee Assessments	2
Extension of time	1
Third Party Objections to Disclosure	1
Breach of Privacy Matters	
General Privacy Breach Complaints	1
Public Body Breach Notifications	2
Other Breach Notifications	1
Comments/Consultations	3
Miscellaneous inquiries/requests/speaking engagements	5
Administrative	1

These numbers do not necessarily correlate to the number of files opened because some files involved two or more issues needing to be addressed.

It is to be noted that the number of breach notifications pursuant to section 49.9 of the Act is down considerably from the nine notifications in 2016/2017. This is not a result of better privacy protections, nor is it a good thing. Rather, it reflects another way in which public bodies are simply not meeting their obligations under the Act. Section 49.9 requires that public bodies that know, or have reason to believe, that a breach of privacy has occurred with respect to the personal information under its control must report the breach to the Information and Privacy Commissioner if the breach is "material". In today's digital world, almost any breach of privacy will amount to a material breach under the Act. I noted in last year's Annual Report that it did not appear that public bodies were recognizing breaches or were not reporting them as required. This does not appear to have improved in 2017/2018. It is important that these reports be made, even if the breach does not seem to be serious. Quite apart from the obvious obligation on public bodies to do so under the legislation, these reports will help to:

a) identify weaknesses or gaps that might lead to future or larger breaches;
b) make employees more aware of what constitutes a breach of privacy, and consequently more careful about avoiding breaches;
c) allow us to learn and improve policies and procedures and build awareness so as to help prevent or avoid similar breaches in other contexts;

Many factors contribute to privacy breaches, not the least of which is human error. The fact that government involves employees dealing with personal information every day means that, even in the best of circumstances, there is going to be more than one material breach of privacy in any one year. Clearly, more education is needed to ensure that all employees understand the obligation to report material breaches of privacy to the Information and Privacy Commissioner.

Twenty-six Review Reports were issued, up from eighteen in 2016/2017.

On the access to information side of matters, the Department of Culture and Heritage was involved in by far the majority of Requests for Review. All of the files with this department files involved a single applicant and all related in one way or another to the discovery of the HMS Erebus and the HMS Terror. The Departments of Finance, Community and Government Services, Health and Justice also were all involved in at least one request to the Office of the Information and Privacy Commissioner (OIPC).

REVIEW REPORTS ISSUED

REVIEW REPORT 17-116

Category of Review:	Breach Notification
Public Body Involved:	Department of Health
Sections of the Act Applied:	Section 49.8, Section 49.9,
Outcome:	Recommendations Accepted

The Department of Health notified the OIPC that an employee had been visiting a home in a community and the occupant of the home showed him the employee's own personal information from his "chart sticker template" which the local health centre uses to label doctor's order forms. The information included the employee's name, date of birth, sex, chart number and NU health care number. The employee was told that the hard drive from which the information had been obtained had been scavenged from a GN computer found at the community dump.

The Information and Privacy Commissioner (IPC) made a number of recommendations, including:

a) that the Department work with CGS to determine what equipment had been replaced in the Health Centre in the community and from there determine exactly what information was on the hard drive;
b) that a system be established to record when computer equipment is replaced and to record the steps taken to destroy the old hard drive in accordance with GN policies and procedures;
c) that steps be taken to recover the hard drive

REVIEW REPORT 17-117

Category of Review:	Breach Notification
Public Body Involved:	Departments of Justice, Health and Community and Government Services
Sections of the Act Applied:	Section 42, Section 40, Section 48
Outcome:	Recommendations accepted but implementation delayed for indeterminate time period

The Department of Justice reported that an employee with the Department of Justice had, inadvertently, been given access to confidential personal health information in the custody of the Department of Health for up to six months and had taken advantage of that access and in at least one instance, disclosed information improperly obtained. The error occurred when the Department of Community and Government Services Helpdesk was asked to approve a Department of Health employee, whose name was similar to the Justice employee, with necessary access to the Y Drive at a community health centre. CGS mistakenly gave access to the Justice employee instead of the Health employee. No one within any of the three departments, other than the Justice employee given unauthorized access, discovered this error until a complaint was received from a member of the public whose information had been improperly collected, used, and disclosed by the Justice employee.

The IPC recommended that CGS change its protocols to include checks and balances to prevent providing inappropriate access to sensitive personal information and that steps be taken as soon as possible to ensure that the electronic information management system used by all GN departments have audit functionalities such as to allow a public body to determine, when necessary, who has had access to files having sensitive personal information.

The IPC also commented that in a situation such as this, where it is clear that an employee had collected, used and disclosed personal health information of a third party, knowing that he had no right to that information, the individual should be prosecuted pursuant to section 59(1) of the act and dismissed, if only to demonstrate to others that

there will be serious consequences for "snooping". In this case, the employee had received only a five-day suspension without pay.

> This was willful behaviour that went on for some length of time and one which involved further disclosure by the employee to members of the community. A five-day suspension does little to telegraph to other employees the seriousness of the offence.
>
> Excerpt from Review Report 17-117

REVIEW REPORT 17-118

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Finance**
Sections of the Act Applied:	**Section 23(1), Section 23(2)(d), Section 23(4)(e), Section 7**
Outcome:	**Recommendations Accepted (except for conducting an *independent* review)**

The Applicant sought access to records concerning the application of the direct appointments policy in place for the GN. The Applicant took the position that the response was incomplete and that the public body had improperly applied Section 23 (unreasonable invasion of privacy).

The IPC commented on the department's "rather appalling" failure to meet its obligations under the ATIPP Act, starting with a double extension of time to respond to the Applicant (which resulted in the identification of less than 300 pages of responsive records), to the inadequacy of the search for records, the "appallingly inconsistent" and "poorly executed" preparation of those records for disclosure and "what can only be described as a lackadaisical response" to the IPC "bordering on disrespectful" in that it took just a

few days short of six months for the department to provide a full response to the review process. She recommended a "full and independent" review of the department's approach to ATIPP, to include a review of the adequacy of resources dedicated to ATIPP, training and corporate culture within the department.

The IPC found that the department did not undertake an adequate search. She recommended that the public body undertake additional searches. She also found that the disclosure of the names of employees named in the course of their employment did not constitute an unreasonable invasion of their privacy and that names, positions and business email addresses of employees should be disclosed. The IPC further found that, because of inconsistent editing, information had been disclosed that had resulted in an unreasonable invasion of the privacy of third parties. She recommended that the third parties involved be advised of the breach and that steps be taken to mitigate, to the extent possible, the damage done by the breaches.

> In dealing with this matter (and, frankly, others in recent months) the department has demonstrated a significant lack of respect for applicants, for the legislation and for this office. This is a concerning trend that needs to be addressed and it can only be addressed by leadership from the Minister, the Deputy Minister and the department's senior staff.
>
> Excerpt From Review Report 17-118

REVIEW REPORT 17-119

Category of Review:	Access to Information / Breach of Privacy
Public Body Involved:	Department of Finance (Human Resources)
Sections of the Act Applied:	Section 12
Outcome:	Recommendations forwarded to the Department and Executive and Intergovernmental Affairs and the Department of Community and Government Services

The Applicant sought information in relation to his job application for a particular position within the GN and, in particular, he asked for access to comments provided by those who acted as his references. The Department of Finance provided the Applicant with some responsive records. In those records were communications between the Department of Finance and the hiring department indicating that one of the interviewers had left his interview notes in another jurisdiction and they could not be found. When asked to look into these lost records, the Department merely referred the Applicant to the hiring department.

The IPC found that there was no evidence to suggest that the Department of Finance held additional records. However, she noted that it was incumbent on the Department, pursuant to section 12 of the Act, to refer the Applicant's inquiries with respect to the missing records to the hiring department. Furthermore, she pointed out that when it came to light that records containing possibly sensitive personal information had gone missing, the matter should have been reported to the IPC pursuant to section 49.9 of the Act. She recommended that steps be taken to create and implement strong policies and procedures on a government-wide basis to address the duty to document.

> Records are made daily which are not on a GN system but which are, none the less, important government records that need to be preserved.
>
> Excerpt from Review Report 17-119

REVIEW REPORT 17-120

Category of Review:	Request to Disregard Request
Public Body Involved:	Executive and Intergovernmental Affairs on its own behalf and on behalf of the Departments of Health, CGS, ED&T, Justice and Finance
Sections of the Act Applied:	Section 53
Outcome:	No Response Required (Authorization Granted in Part)

The Department of Executive and Intergovernmental affairs made an application on its own behalf and on behalf of five other departments, asking for authorization pursuant to section 53 of the Act to disregard requests for information received on a particular date from a particular Applicant. In making the request, it was noted that the Applicant in question had made numerous previous requests for information, all in relation to the same subject matter of the current request and had received thousands of pages of records. In addition, documents had been disclosed to the Applicant in the course of an ongoing litigation between the GN and the Applicant. In short, they argued that the Applicant had already received all records responsive to the matters in question.

The IPC found that, in the particular circumstances of this case, the Applicant had over-stepped by directing his Request for Information to six public bodies when only one would have any responsive records. She also found that the request in question was in the form of questions and was not a request for "records". She allowed all but one of the public bodies to disregard the Applicant's request and recommended the disclosure of specific records requested, if they existed and if they had not already been disclosed either in the litigation discovery process or under a previous ATIPP request.

REVIEW REPORT 17-121

Category of Review:	Access to Information
Public Body Involved:	Nunavut Housing Corporation
Sections of the Act Applied:	Section 22
Outcome:	Recommendations largely not accepted

The Applicant, an unsuccessful candidate for a position within the Nunavut Housing Corporation, requested access to all records in relation to the job competition in which he was mentioned. The Nunavut Housing Corporation denied access to all responsive records pursuant to section 22 of the Act which allows public bodies to withhold information "that is evaluative or opinion material compiled solely for the purpose of determining the applicant's suitability, eligibility or qualifications for employment" when that information has been provided implicitly or explicitly in confidence. This was notwithstanding that both individuals who provided references for the Applicant acknowledged that the Applicant would be able to review the information through the ATIPP process.

The IPC found that the public body had misinterpreted section 22 of the Act and that much of the information contained in the responsive records should have been disclosed. She recommended the disclosure of most of the records.

> There is no automatic exemption for the content of reference checks. Nor can the public body give any referee assurances that their comments will be held in confidence. Such assurances are not possible under the Act.
>
> Excerpt from Review Report 17-121

REVIEW REPORT 17-122

Category of Review:	**Access to Information – Deemed Refusal**
Public Body Involved:	**Department of Finance**
Sections of the Act Applied:	**Section 8(2)**
Outcome:	**Recommendations accepted in spirit**

The Applicant made a Request for Information to the Department of Finance on December 13, 2016. When he had not received a response by January 24th, he asked for a review by the IPC on the basis of a deemed refusal. The IPC asked the Department to provide an explanation four times over the course of January, February and March of 2017 for an explanation. No response was received to any of those letters until March 22nd at which time the department indicated that it had not properly handled the request and that they had not yet initiated the response process but that it would be commenced forthwith. In early May, the Applicant advised the IPC that he had still not received a response. The response was finally sent to the Applicant on May 10th, almost 120 days after the request had been made.

The IPC found that the Department of Finance had failed completely to meet its responsibilities under the Act. She recommended that the department:

a) immediately undertake a review of the resources and manpower realistically necessary to maintain compliance of ATIPP responsibilities;
b) review and create a clear step by step process for the handling of ATIPP requests and obtain appropriate software to assist in tracking each ATIPP request and Request for Review received, including appropriate reminders generated from time to time to ensure that ATIPP staff remain on top of responses.
c) consider removing ATIPP responsibilities from the current ATIPP Co-Ordinator's job description and giving them to someone else within the department with sufficient time to properly deal with ATIPP matters.

> It is not an excuse, under the Act, that the ATIPP Co-Ordinator has responsibilities unrelated to ATIPP to complete. The deadlines under the ATIPP Act are legislative in nature and must, therefore, be given higher priority than other deadlines which are more artificially imposed.
>
> Excerpt from Review Report 17-122

REVIEW REPORT 17-123

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Community and Government Services**
Sections of the Act Applied:	**Section 24(1), Section 15, Section 1, Section 5**
Outcome:	**Recommendations not followed**

The Applicant made a request for information in relation to a particular tender for a job in a small community, including all successful and unsuccessful bids. The Department responded with a number of records but the Applicant felt that there were missing records. In the course of the review, it came to light that the pubic body had identified additional records but had withheld them pursuant to section 24 and section 15 of the Act without advising the Applicant about the existence of these records. With respect to some of the records, they argued that the request was for emails "within" CGS and that, therefore excluded emails with individuals in another department. Again, they did not let the Applicant know that the records existed. Further, they decided that the Applicant did not need some records because the same information was contained in other records which were disclosed.

The IPC found that the public body had not established that the information withheld pursuant to section 24 met the criteria for such an exception. With respect to section 15, she found that most of the records could be disclosed without revealing anything subject to solicitor/client privilege. She also chastised the department for its very narrow

interpretation of the Request for Information and for not disclosing the existence of some records. She recommended the disclosure of most of the responsive records and that new searches be done to ensure all of the responsive records had been identified.

> It is not for the public body to assume or surmise or conclude what issue the applicant is seeking to confirm and it is certainly not for the public body to decide that they have disclosed "enough" information to satisfy an applicant's curiosity. The purpose of the applicant's request is of no relevance whatsoever to the response given. If there are records that are responsive to a request, they must be disclosed, subject only to the exceptions set out in the act.
>
> Excerpt from Review Report 17-123

REVIEW REPORT 17-124

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Human Resources**
Sections of the Act Applied:	**Section 22**
Outcome:	**Recommendations not followed**

The Applicant applied for a position with the GN but failed to get the job after the public body did reference checks for him. The Applicant sought to obtain copies of records in relation to the reference checks. The public body denied access pursuant to section 22 of the Act arguing that referees are given the "option to declare whether they would like the evaluative and opinion portion of the reference check to be confidential" and that when the answer is "yes" there is a blanket policy to deny the Applicant access. They further argued that the intent of providing referees "the opportunity to declare some information confidential is to help ensure that the Government of Nunavut (GN) receives honest and accurate accounts regarding the conduct and performance of prospective

employees, without fear of intimidation and reprisal" whether or not they are in a position of seniority to the job applicant.

The IPC found that the *Access to Information and Protection of Privacy Act*, being quasi-constitutional in nature, takes precedence over any GN policy and there cannot be a blanket policy which directs that evaluative information collected on an employment reference check will never be disclosed to an Applicant where there has been a request for confidentiality. She further found that to the extent that the GN policy is to advise referees that they may "choose" confidentiality, that advice is contrary to the Act. The IPC recommended the revision of Directive 511 so as to reflect the law and to change the caution given to those providing references to reflect the possibility that, notwithstanding a request for confidentiality, the information may be disclosed to the job candidate. The IPC further recommended that in this case, the public body reconsider its refusal to disclose large portions of the responsive records which consisted of the Applicant's own personal information.

REVIEW REPORT 17-125

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Finance**
Sections of the Act Applied:	**Section 23**
Outcome:	**Recommendations not accepted**

The Applicant made a request to the Department of Finance for a list of all GN positions with base salaries of $100,000.00 or more, the positions held and the names of the current incumbents as of April 1, 2017. The public body indicated they were unable to disclose the information requested because that would constitute an unreasonable invasion of the privacy of those employees.

While the IPC agreed that section 23(2)(f) raises a presumption that the disclosure of information will arise if the information describes a third party's finances, income, assets, or other financial information, section 23(4)(e) provides that it is NOT an

unreasonable invasion of privacy to disclose information that relates to the third party's classification, salary range or employment responsibilities as an officer or employee of a public body. The IPC recommended the disclosure of all positions for which the starting base salary is in excess of $100,000.00, the name of the current incumbent in each such position and the salary range for each such position.

REVIEW REPORT 17-126

Category of Review:	**Access to Information - Fees**
Public Body Involved:	**Department of Justice**
Sections of the Act Applied:	**Section 5(3), Regulations 9, 10, 11, 14**
Outcome:	**Recommendation to Reassess Fee Accepted** **No Waiver of Fees on Reassessment**

The Applicant requested information in relation to inmate complaints over a five-year period from three named correctional facilities. The public body provided the Applicant with a fee estimate in excess of $4,000. The Applicant sought a fee waiver but the department declined. The Applicant requested a review of both the fee assessed and the decision to refuse to waive the fee.

The IPC found that the Act contemplated the payment of fees for those seeking access to public records where the cost of the fees, calculated in accordance with the regulations, is in excess of $150.00. She accepted that the fee estimate provided was in accordance with the regulations. She found, however, that the public body failed to consider the public interest in disclosure. She recommended that the public body reconsider the Applicant's request for a fee waiver on the basis of the public interest in disclosure, completely separate from any financial considerations, keeping in mind the stated purpose of the Act of making pubic bodies more accountable to the public.

REVIEW REPORT 17-127

Category of Review:	Access to Information
Public Body Involved:	Department of Culture and Heritage
Sections of the Act Applied:	Section 2, Section 3
Outcome:	- Recommendation to conduct further searches not followed - Appealed to the Nunavut Court of Justice (Appeal pending) - Recommendation to review and amend policies referred to CGS and EIA for review

The Applicant made many Requests for Information from the Department of Culture and Heritage, resulting in many Requests for Review to the OIPC. In each case, one of the issues on review was whether the public body had undertaken an adequate search for records. The records showed that some employees had been using personal email addresses and personal devices to communicate with respect to departmental business but no search was done of those accounts or devices for records that might be responsive to the requests for information.

The IPC found that there were many communications written from personal email accounts, and perhaps from personal devices that were clearly about a subject within the employee's job description and which were sent or received by the employee in his capacity as a GN employee. As such, such records are "under the control" of the public body and that any such records were subject to an access to information request as a result. She found that where there is a reasonable possibility that an employee has used a personal device and/or email address or a social media account to address issues within the employee's job responsibilities, it is incumbent on the public body to produce those records in response to an ATIPP request. She recommended that the Department of Culture and Heritage conduct a search for additional records which might exist in the private accounts of the employees in question. She further commented on the lack of any policies with respect to the use of personal devices or accounts for the purpose of doing GN business and recommended that this public body immediately develop a comprehensive policy in this regard, to include a prohibition of the use of such means of

communication except in exigent circumstances. She further recommended that the GN conduct a review of all existing policies in relation to the use of electronic communications and that amendments be made to clarify the intended purposes of each policy and to correct errors and that a new policy be developed on a government-wide basis to address the use of personal devices.

REVIEW REPORT 17-128

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 3, Section 7**
Outcome:	**Recommendation not accepted**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 20 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts.

The IPC found that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done.

REVIEW REPORT 17-129

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7**
Outcome:	**No Recommendation made**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 12 pages of records. The

Applicant requested a review on the basis that the public body had failed to search all relevant records.

The IPC found that there was nothing to suggest that the search done by the department was not thorough. She found that while section 7 places a positive onus on public bodies to make every reasonable effort to assist an Applicant and to respond openly, accurately, completely and without delay, that burden had been met in this case and there was no evidence that any records were missing from the response provided.

REVIEW REPORT 17-130

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 13(1)(a), Section 15(a)**
Outcome:	**- Recommendation with respect to sections 7 and 15 not accepted** **- Recommendations with respect to section 13**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 70 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. The Applicant also requested a review of those parts of the records that were withheld pursuant to sections 13 (information the disclosure of which would reveal a confidence of the Executive Council) and 15(a) (information subject to solicitor/client confidence).

The IPC found that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done. She further found that those items redacted pursuant to section 13(1) did not meet the criteria for an exception under that section and recommended these items be disclosed.

Finally, she agreed with the public body that the information redacted pursuant to section 15(a) was protected by solicitor/client privilege but that the public body had failed to properly exercise its discretion with respect to disclosure. She recommended that the public body actively exercise its discretion.

> There may well be good reasons for the department in this case to refuse to disclose the information protected by solicitor/client privilege, but they must consider both options. I therefore **recommend** that the public body actively exercise its discretion with respect to these five records and provide the Applicant with an explanation for their decision if their decision is not to disclose the records.
>
> Excerpt from Review Report 17-130

REVIEW REPORT 17-131

Category of Review:	Access to Information
Public Body Involved:	Department of Culture and Heritage
Sections of the Act Applied:	Section 7, Section 14(1)(a), Section 15(a), Section 16(1)(a), Section 20
Outcome:	- Recommendation with respect to section 7 not accepted - Recommendations with respect to section 14 and 16 accepted - Recommendation with respect to section 15 partially accepted - Recommendation with respect to section 20 accepted but for other reasons

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 170 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those

other email accounts. In addition, he objected to information withheld pursuant to sections 14(1)(a) (disclosure could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options developed for a public body), 15(a) (solicitor/client privilege), 16(1)(a) (disclosure could reasonably be expected to impair relations between the GN and the Government of Canada) and 20(1) (disclosure would prejudice a law enforcement matter).

The IPC found:

a) with respect to section 7, that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;
b) with respect to section 14, that some of the information redacted pursuant to this section met the criteria for such an exception, but other information did not. She recommended the active exercise of the public body's discretion with respect to those items that met the criteria and that those items that did not meet the criteria be disclosed;
c) with respect to those sections redacted pursuant to section 15, that most of the information redacted on the basis of solicitor/client privilege met the criteria for the exception, but noted that in most cases there was no indication that the public body had actively exercised its discretion with respect to disclosure. For these items, she recommended the active exercise of discretion. There were portions of some records redacted pursuant to this section that did not meet the criteria. The IPC recommended that these items be disclosed;
d) with respect to section 16, that there was no evidence that the disclosure might impair relations between the GN and the Government of Canada and that the content of the records involved were insufficient to convince her that the intergovernmental relationship would be negatively affected by the redacted information. She recommended that the information be disclosed
e) with respect to section 20(1)(a), that there was nothing to suggest a reasonable possibility that the disclosure of the information in question might prejudice a law

enforcement matter and recommended that the redacted information be disclosed.

REVIEW REPORT 17-132

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 14(1)(a), Section 15(a), Section 16(1)(a), Section 20**
Outcome:	**No Response Received (more than 7 months past due)**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 110 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. In addition, he objected to information withheld pursuant to sections 14(1)(a) (disclosure could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options developed for a public body), 15(a) (solicitor/client privilege), 16(1)(a) (disclosure could reasonably be expected to impair relations between the GN and the Government of Canada) and 20(1) (disclosure would prejudice a law enforcement matter).

The IPC found:

a) with respect to section 7 that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;
b) with respect to section 14, that some of the information redacted pursuant to this section met the criteria for such an exception, but other information did not. She recommended the active exercise of the public body's discretion with respect to

those items that met the criteria and that those items that did not meet the criteria be disclosed;

c) With respect to those sections redacted pursuant to section 15, that most of the information redacted on the basis of solicitor/client privilege met the criteria for the exception, but noted that there was no indication that the public body had actively exercised its discretion with respect to disclosure. For these items, she recommended the active exercise of discretion. There were also some records redacted pursuant to this section that did not meet the criteria. The IPC recommended that these items be disclosed;

d) With respect to section 16, that there was no evidence that the disclosure might impair relations between the GN and the Government of Canada and recommended that the information be disclosed

e) With respect to section 20(1)(a), that there was nothing to suggest a reasonable possibility that the disclosure of the information in question might prejudice a law enforcement matter and recommended that the redacted information be disclosed.

REVIEW REPORT 17-133

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 13(1)(a), Section 14(1)(a), Section 15(a), Section 16(1)(a)(i), Section 16(1)(a)(ii) and Section 16(1)(c)**
Outcome:	**- Recommendation with respect to section 7 not accepted** **- Recommendations with respect to remaining sections largely accepted**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 275 pages of records. The Applicant pointed out the use of personal email addresses and requested a review

on the basis that public body should have searched for responsive records in those other email accounts. In addition, he objected to information withheld pursuant to sections 13(1)(a) (disclosure would reveal a confidence of the Executive Council), 14(1)(a) (disclosure could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options developed for a public body), section 14(a)(f) (disclosure would reveal the content of agendas or minutes of meetings),15(a) (solicitor/client privilege), and 6(1) (disclosure could reasonably be expected to impair relations between the GN and the Government of Canada).

The IPC found:

a) with respect to section 7 that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;
b) with respect to section 13(1)(a), that the section was properly applied to some of the information redacted pursuant to this section, but improperly applied to other information. She recommended the disclosure or reconsideration under other provisions of the Act to that information that did not meet the criteria for an exception pursuant to this section;
c) with respect to section 14(1)(a), that some of the information redacted pursuant to this section met the criteria for such an exception, but other information did not. She recommended the active exercise of the public body's discretion with respect to those items that met the criteria and that those items that did not meet the criteria be disclosed;
d) with respect to section 14(1)(f), that none of the information redacted met the criteria for an exception pursuant to this subsection. She recommended the disclosure of all information redacted pursuant to this subsection with the exception of the names of several private citizens;
f) with respect to those sections redacted pursuant to section 15, that some of the information redacted on the basis of solicitor/client privilege met the criteria for the exception, but noted that there was no indication that the public body had

actively exercised its discretion with respect to disclosure. For these items, she recommended the active exercise of discretion. There were also some records redacted pursuant to this section that did not meet the criteria. The IPC recommended that these items be disclosed;

g) With respect to section 16, that for most of the records this was applied to there was no evidence that the disclosure might impair relations between the GN and the Government of Canada. She recommended the disclosure of most of the information redacted pursuant to this section.

> Section 15 is also a discretionary exception. Therefore, not only must the material redacted fit the criteria for an exemption, the public body must then exercise its discretion and decide whether or not to disclose the record in question.
>
> Excerpt from Review Report 17-133

REVIEW REPORT 17-134

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7**
Outcome:	**Recommendations not accepted**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 16 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. The IPC found that that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to

extend their searches to include those accounts. She recommended that these additional searches be done.

REVIEW REPORT 17-135

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 13(1)(a), Section 15(a), Section 20(1)(a)**
Outcome:	**- Recommendation with respect to section 7 not accepted** **- Recommendation with respect to section 20 accepted but for other reasons;** **- Recommendations with respect to remaining sections largely accepted**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 16 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. The Applicant further objected to the withholding of information pursuant to sections 13(1)(a) (cabinet confidence), section 15(a) (solicitor/client privilege) and section 20(1)(a) (disclosure prejudicial to a law enforcement matter).

The IPC found:

a) with respect to section 7 that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;
b) with respect to section 13(1)(a), that the section was properly applied to some of the information redacted pursuant to this section, but improperly applied to other information. She recommended the disclosure or reconsideration under other

provisions of the Act to that information that did not meet the criteria for an exception pursuant to this section;

c) with respect to those sections redacted pursuant to section 15, that some of the information redacted on the basis of solicitor/client privilege met the criteria for the exception, but noted that there was no indication that the public body had actively exercised its discretion with respect to disclosure. For these items, she recommended the active exercise of discretion. There were also some records redacted pursuant to this section that did not meet the criteria. The IPC recommended that these items be disclosed;

d) With respect to section 20(1)(a), that there was nothing to suggest a reasonable possibility that the disclosure of the information in question might prejudice a law enforcement matter and recommended that the redacted information be disclosed.

REVIEW REPORT 18-136

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 23(1), Section 15(a), Section 19(b), Section 16(1)(a), Section 13(1)(a), Section 14(1)(b)**
Outcome:	**- Recommendation with respect to section 7 not accepted** **- Recommendations with respect to remaining actions largely accepted**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 168 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. The Applicant further objected to the withholding of information pursuant to sections 23(1) (disclosure would result in unreasonable invasion of third party privacy), section 15(a) (solicitor/client privilege), section 19(b) (disclosure would result in damage to or interfere with conservation sites), section 16(1)(a) (impairment to

intergovernmental relationships), section 13(1)(a) (disclosure would reveal cabinet confidence) and section 14(1)(b) (disclosure would reveal advice to officials).

The IPC found:

a) with respect to section 7 that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) with respect to section 23, that some of the information redacted was appropriate but that the disclosure of business contact information does not, in most situations, amount to an unreasonable invasion of privacy. She recommended the disclosure of some of the redacted information;

c) with respect to those sections redacted pursuant to section 15, that most of the information redacted on the basis of solicitor/client privilege met the criteria for the exception, but noted that there was no indication that the public body had actively exercised its discretion with respect to disclosure. For these items, she recommended the active exercise of discretion. There were also some records redacted pursuant to this section that did not meet the criteria. The IPC recommended that these items be disclosed;

d) with respect to section 19, the IPC found that the information in question was clearly about the location of sites having anthropological and/or cultural significance. There was no evidence, however, that the disclosure of this particular information would result in harm, in particular because the redacted information is already available to the public with a simple internet search. She recommended the disclosure of most of the redacted information;

e) with respect to section 16(1)(a), the IPC found that there was nothing offered by the department to support a conclusion that the disclosure of the redacted material could reasonably be expected to impair an intergovernmental relationship. She did find as well that some of the redacted information constituted a consultation pursuant to section 14(1)(b) and that it should be assessed on that basis;

f) with respect to section 13(1)(a), the IPC found that the redacted information did not meet the criteria for the exception and recommended that this information be disclosed;

g) with respect to section 14(1)(b), the IPC found that the redacted information met the criteria for the exception but that there was no evidence that any discretion had been exercised. She recommended that the public body actively exercise its discretion with respect to each of these redactions;

REVIEW REPORT 18-137

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7**
Outcome:	**No Response Received (more than 4 months past due)**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 199 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. He also suggested that there were missing records, including records referred to as “attachments” in a number of emails, and questioned the thoroughness of the search of GN records.

The IPC found:

a) that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) that there did appear to be a gap in responsive records for 2016 and recommended that additional searches be conducted;

c) that there may be some missing attachments and recommended that additional searches be conducted for these

REVIEW REPORT 18-138

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 15(a)**
Outcome:	**- Recommendation with respect to section 7 not accepted** **- Recommendations with respect to section 15 accepted but no discretion exercised**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 99 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. The Applicant further objected to the withholding of information pursuant to section15(a) (solicitor/ client privilege).

The IPC found:

a) with respect to section 7 that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) with respect to section 15(a) that all of the redacted information met the criteria for an exception pursuant to this section, but that there was no evidence that the public body had actively exercised its discretion. She recommended that the public body actively and visibly exercise its discretion.

REVIEW REPORT 18-139

Category of Review:	Access to Information
Public Body Involved:	Department of Culture and Heritage
Sections of the Act Applied:	Section 7
Outcome:	No Response Received (More than four months past due)

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 140 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. He also suggested that some of the attachments referred to in the responsive emails had not been provided and that there were other missing records.

The IPC found:

a) that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) that there did appear to be a gap in responsive records for 2016 and recommended that additional searches be conducted;

c) that there may be some missing attachments and recommended that additional searches be conducted for these.

> While much of our day to day work is done via email and a search of email records is likely to identify the vast majority of responsive records in most cases, it is not sufficient to search only email records. The onus is on the public body to show that they have searched **all** relevant records.
>
> Excerpt from Review Report 18-139

REVIEW REPORT 18-140

Category of Review:	Access to Information
Public Body Involved:	Department of Culture and Heritage
Sections of the Act Applied:	Section 7, Section 15(a)
Outcome:	- Recommendation with respect to section 7 not accepted - Recommendations with respect to section 15 accepted but no discretion exercised

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 111 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts. He also suggested that some of the attachments referred to in the responsive emails had not been provided and that section 15(a) had been improperly applied to some of the records.

The IPC found:

a) that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) that there may be some missing attachments and recommended that additional searches be conducted for these;

c) with respect to section 15(a) that all of the redacted information met the criteria for an exception pursuant to this section, but that there was no evidence that the public body had actively exercised its discretion. She recommended that the public body actively and visibly exercise its discretion.

REVIEW REPORT 18-141

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7, Section 15(a)**
Outcome:	**No Response Received (more than 4 months past due)**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 201 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts that there were missing records, including records referred to as "attachments" in a number of emails, and questioned the thoroughness of the search of GN records. Finally, he objected to the application of section 15(a) to some of the records.

The IPC found:

a) that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) that there may be some missing attachments and recommended that additional searches be conducted for these;

c) with respect to section 15(a) that all of the redacted information met the criteria for an exception pursuant to this section, but that there was no evidence that the public body had actively exercised its discretion. She recommended that the public body actively and visibly exercise its discretion.

REVIEW REPORT 18-142

Category of Review:	**Access to Information**
Public Body Involved:	**Department of Culture and Heritage**
Sections of the Act Applied:	**Section 7**
Outcome:	**No Response Received (more than 4 months past due)**

The Applicant requested certain records in relation to the discovery of the HMS Terror and the HMS Erebus. The department identified and disclosed 375 pages of records. The Applicant pointed out the use of personal email addresses and requested a review on the basis that public body should have searched for responsive records in those other email accounts that there were missing records, including records referred to as "attachments" in a number of emails, and questioned the thoroughness of the search of GN records.

The IPC found:

a) that where it is clear that an employee has used a personal account to conduct GN business, there is an obligation on the public body to extend their searches to include those accounts. She recommended that these additional searches be done;

b) that there did appear to be a gap in responsive records and recommended that additional searches be conducted;

c) that there may be some missing attachments and recommended that additional searches be conducted for these.

> I found that all business-related communications were "under the control" of the GN and therefore, subject to the *Access to Information and Protection and Privacy Act* wherever they existed, whether that be on a GN system or on an employee's personal device or in an employee's personal email account.
>
> Excerpt from Review Report 18-142

TRENDS AND ISSUES – MOVING FORWARD

Nunavut is the only jurisdiction in Canada not addressing the need to update and modernize its *Access to Information and Protection of Privacy Act*. It is also the only jurisdiction in Canada that does not have health specific privacy legislation. As I noted in last year's Annual Report, there are advantages to being the last to do something. It allows us to learn from others and to gather the best from the work others have done. But this work must be done. Nunavummiut deserve to have modern and effective legislation to assist them to participate in the government that they have created and to ensure that their personal information and personal health information is not being inappropriately collected, used or disclosed by public bodies. While there have been some piecemeal amendments to the legislation, including amendments to address some longstanding recommendations from the Information and Privacy Commissioner, what is really needed is a thorough review, with independent advice and direction so that it can continue to allow for the right of access and the protection of privacy with the new realities in mind. I have provided a starting point with the report submitted to the Standing Committee on Oversight of Government Operations and Public Accounts last summer. Now steps must be taken to move this forward.

Perhaps more importantly, as noted in the opening message to this Annual Report, there has been a marked and noticeable decline in public bodies' adherence to and respect for the values of the *Access to Information and Protection of Privacy Act*. Legislation without leadership achieves nothing. It is time for senior management to take an ownership role in promoting both adherence to the legislated duties imposed by the Act, but also in encouraging all employees to comply with the spirit and intention of the legislation. The mindset at the managerial level must be to aim to disclose as much information as possible rather than looking for ways to avoid disclosure. And there must

be much more of a focus on protecting the privacy of Nunavummiut and in considering the privacy implications of what government does on a day to day basis.

Review of Policies

In Review Report 17-127, I made did a review of all GN policies I could find with respect to the use of electronic records and found them scattered, disparate, poorly written, unclear and, for the most part not complete. In one case, there appeared to be a typographical error which changed the meaning of the policy completely. In another, there was reference to a piece of legislation (the *Records Management Act*) which does not exist in Nunavut. There was nothing in any of the numerous policies relating to electronic records that dealt with the reality that employees use their own personal email accounts and their own personal devices to conduct government business. During the course of the review I was advised that a policy was being developed which would classify all text and IM messages as "transitory" in nature. This is a dangerous and inappropriate policy for the purposes of ensuring an accurate record of decision making communications. I recommended:

a) that there be a review of all the policies in relation to the use of electronic communications and that amendments be made as necessary to clarify the intended purposes of each such policy and to correct errors;

b) that a new and separate policy be developed to specifically address the issue of the use of personal devices and email accounts for undertaking GN business which will be applicable to all GN employees and that the policy should include:

   a. a prohibition on the use of privately owned equipment and accounts as a means of communication except in exigent circumstances;
   b. provisions for clear directions with respect to the management of such communications where such communications are necessary;

c. the following paragraph from the existing Acceptable Use of Mobile Devices Policy:

> All GN wireless communications records shall be subject to all laws, policies and procedures that apply to the management of any other GN information or record. As per the *Archives Act* every decision and communication with respect to GN-related business must be documented and accessible based on records management retention schedules and/or under the provisions of the *Access to Information and Protection of Privacy Act*.

d. providing for significant and specific consequences for failure to comply with the policy

c) that steps be taken to disseminate and enforce this policy government-wide such that there can be no question that every GN employee is aware of both the policy and consequences that might apply in the event of failure to comply;

While these recommendations were said to be forwarded to the Department of Community and Government Services and the Department of Executive and Intergovernmental Affairs, I have heard nothing further from either of these departments and it is unclear whether such a review and revision is being undertaken. For that reason, I make the same recommendations here.

Focus on File Management

Along similar lines, in last year's Annual Report I discussed the fact that file management has not kept up with the way government works today. There are few, if any file management professionals working in government any more. Unlike the paper world, every employee with a computer has control over his or her electronic records with little or no training or checks and balances. As an inevitable result, file management and record keeping are becoming more haphazard and unwieldly. Quite apart from the need to maintain good records for current and future use, there is a direct relationship between good records and information management and the ability of a public body to

meet its responsibilities under the *Access to Information and Protection of Privacy Act*. Good records and information management practices can prevent records from being lost or misfiled, or from being improperly deleted. At the same time, strong records and information management practices will reduce the time and effort required to identify and gather records in response to an access request. More resources and focus need to be committed to this basic function of government - good, consistent and monitored record keeping.

Adequate Resources

This is another repeat of an issue raised in my last Annual Report. Even perfect legislation will fail if there are inadequate resources to meet the demand. At one point during the year, the ATIPP Coordinator in the Department of Finance was very candid in telling me that, when combined with his other duties, he was unable to meet his responsibilities under the Act. Because Finance includes all Human Resources matters, it will inevitably receive a more access to information requests than most other departments. Furthermore, it holds significant amounts of personal information and it will, therefore, also likely receive more privacy breach complaints and have to deal with more inadvertent privacy breaches than most departments. Other departments are similarly challenged. More resources need to be dedicated to access and privacy in public bodies. Access to Information is client driven. There is a very real ebb and flow to the volume of work as a result. That said, when the tide is high, public bodies need to have the resources and the flexibility to deal with whatever comes in the door. This includes, where appropriate, a full-time position to deal with ATIPP matters and sufficient numbers of employees trained so that when the main ATIPP Coordinator in a department goes on holidays or is away for some other reason, there is someone who can be assigned to do the necessary work. Ensuring adequate resources is part of the leadership required to allow the *Access to Information and Protection of Privacy Act* work the way it was intended.

Education

As noted in my opening comments, education is a key for our children to learn to use the electronic resources that their generation will offer while being able to protect their privacy at the same time. This generation will "live" on-line and they have to be given the tools, starting a very young age, to do that safely. They need to be able to recognize the way in which their personal information is being mined and used so that they can make intelligent choices. We are behind the curve on ensuring that necessary education. That said, a lot of work has been done to develop appropriate age-level educational materials and course outlines. One of the projects that my counterparts from across the country and I have taken on is to create some basic lesson plans for this purpose. Three of these lesson plans have recently been published and these can be found on my website under the heading "Resources". More needs to be done by the Department of Education to ensure that children start to learn about the value of their privacy, how to protect privacy on-line and how to deal with on-line bullying. This education has to begin right from the age of kindergarten and continue all the way through to Grade 12. I would encourage the Government of Nunavut to ensure that this education is embedded in the curriculum for all grades as soon as possible.