CHAPTER 3

PART 3 – ACCESS TO INFORMATION

DIVISION 1 – APPLICATION OF THIS PART

DIVISION 2 – OPEN ACCESS INFORMATION

DIVISION 3 – REQUEST FOR ACCESS TO INFORMATION

DIVISON 4 – PROCESSING OF ACCESS REQUEST

DIVISION 9 – INFORMATION TO WHICH ACCESS MAY BE DENIED

DIVISON 10 – PUBLIC INTEREST OVERRIDE AND MANDATORY DISCLOSURE

CHAPTER 3 OVERVIEW

There are two types of exceptions under the *Act* – **mandatory exceptions** and **discretionary exceptions**.

Division 8 – Mandatory exceptions

Mandatory exceptions begin with the phrase "the head of a public body *must* refuse to disclose." If information falls within a mandatory exception, a public body must refuse to disclose all or part of the record as required. Public bodies must review all of the criteria and weigh all of the relevant factors relating to a mandatory exception before deciding whether the exception applies. The only case where information that falls within a mandatory exception can be disclosed is where **section 82** of the *Act* requires disclosure in the public interest. In this case **section 82** overrides the exception.

Division 9 – Discretionary exceptions

Discretionary exceptions to the right of access permit a public body to decide whether or not to withhold all or part of a record. Discretionary exceptions commence with the phrase "the head of a public body **may** refuse to disclose." The exercise of discretion is fundamental to applying the *Act*. It requires the head, or staff member delegated to exercise the discretion of the head, to weigh all factors in determining whether or not information that qualifies for a discretionary exception should be withheld. The public body must be able to show that the records were reviewed, that all relevant factors were considered and, if the decision is to withhold the information, that there are sound reasons to support the decision.

Harms test - Some exceptions (both mandatory and discretionary) are based on a harms test. This generally provides that access to all or part of a record may or must be refused if disclosure could reasonably be expected to harm a particular public or private interest. The general test for harm under the *Act* is whether there is a reasonable expectation of harm flowing from disclosure of the specific information at issue.

The evidence must demonstrate a probability of harm from disclosure and not just a well-intentioned but unjustifiably cautious approach to the avoidance of any risk whatsoever because of the sensitivity of the matters at issue. The likelihood of harm must be genuine and conceivable.

PART 3

D1

DIVISION 1 – APPLICATION OF THIS PART

SECTION 38 Generally excluded information

A basic principle of the *ATIPP Act* is to give the public access to the records of a public body. Section 38 explains the various exceptions that require or allow a public body to identify records that are not subject to the access part of the *Act*. Any exceptions to the right of access should be applied in a limited and specific way to provide as much access to information as possible.

"GENERALLY EXCLUDED INFORMATION" means the information and records described in paragraphs 38(1)(a) to (o).

Subsection (1) provides that Part 3 (access to information) does not apply to these types and classes of information and records even if held by a public body.

> **38(1)** This Part applies to all information and records (including court services information) held by a public body except the following:
>
> **(1)(a)** a court record;
>
> **(1)(b)** information contained in a court registry;
>
> **(1)(c)** judicial information

"COURT RECORD" means a record contained in a court registry, or that is created or produced by or for a court in respect of a proceeding, and includes:

a. a record of the dates on which the proceeding was heard or will be heard and the name of the judge who heard or is listed to hear the proceeding,

b. a record of a judgement in respect of the proceeding, including an order made or a direction given by the judge during the proceeding, and

c. a record admitted into evidence by the court during the proceeding.

"COURT REGISTRY STAFF" means the employees of a public body who provide support services to a judge or a court.

"COURT SERVICES INFORMATION" means information about a program or activity of a public body that provides support services to a court and includes information about employment matters in respect of court registry staff but does not include judicial information or a court record.

"JUDICIAL INFORMATION" means:

a. Information collected, used, stored, processed or generated by a judge, or an individual working for or on behalf of the judge;

b. information about a judge, including
   i. information about the support services provided to the judge by court registry staff,
   ii. information about the judge's schedule in relation to proceedings;
   iii. information about the judge's judicial training program;
   iv. information about the judicial activity of the judge, including statistics about the activity prepared by or for the judge, and

c. information about, and the records of, the Judicial Council of the Territorial Court (established under the *Territorial Court Act*), including information and records related to the duties and powers of a member of the Judicial Council of the Territorial Court.

"JUDGE" means a judge, deputy judge or justice of the court. This definition supports further defining the scope of judicial information and the scope of this exception provision.

(1)(d) adjudicative information;

"ADJUDICATIVE INFORMATION" means information collected, used, stored, processed or generated by an adjudicator, or an individual working for or on behalf of an adjudicator, in respect of a proceeding over which the adjudicator is presiding or has presided but does not include a decision (including reasons) or order made, or a direction given, by the adjudicator in respect of the proceeding.

"ADJUDICATOR" means a person or body (other than a court) that is authorized under an act of the Legislature or of Parliament to hear and determine a matter brought before them and may, on conclusion of the hearing make a decision that is legally-binding on a person whose rights are or may be affected by the decision.

(1)(e) a record made by or for a member of the Legislative Assembly who is not a minister;

(1)(f) a record made by or for a member of the Legislative Assembly who is a minister that relates to a personal or constituency matter of the member;

These provisions exclude the application of a record of a Member of the Legislative Assembly (MLA).

It is important for the Office of a Minister to have a process in place to separate records of their responsibilities as a Minister of their appointed departments, from records that they receive or create as a Member of the Legislative Assembly.

"CABINET RECORDS" are records created or received that reflect meetings of Cabinet, Management Board, or Cabinet Committees.

"MINISTERIAL RECORDS" are records created or received by a Minister as part of his or her ministerial portfolio.

"MINISTER RESPONSIBLE", for a department, means the minister appointed under the *Government Organization Act* to preside over the department.

Cabinet and Ministerial records are **public records** subject to the provisions of the *ATIPP Act* and the *Archives Act*.

> **(1)(g)** a record made by or for an officer of the Legislative Assembly that relates to their exercise of powers or their performance of duties under an Act;

"OFFICER" of the Legislative Assembly means:

a. the Commissioner,

b. the Ombudsman (appointed under the Ombudsman Act),

c. the Chief Electoral Officer (appointed under the *Elections Act*),

d. the Child and Youth Advocate (appointed under the *Child and Youth Advocate Act*),

e. an Individual appointed under the *Conflict of Interest (Members and Ministers) Act* as a member of the Conflict of Interest Commission,

f. the Public Interest Disclosure Commissioner (appointed under the *Public Interest Disclosure of Wrongdoing Act*), and

g. any other individual appointed under an act as an officer of the Legislative Assembly.

In some jurisdictions, the Speaker and the Clerk of the Legislative Assembly are included in this category. In Yukon's case, they have not been included because Yukon's Legislative Assembly

custom is to treat the Speaker and the Clerk as presiding officers and not 'House' officers like those officers included in this category.

"OMBUDSMAN" means (a) the individual appointed as the Ombudsman under the *Ombudsman Act*, or (b) an individual appointed as an acting Ombudsman under the *Ombudsman Act*.

> **(1)(h)** a record that relates to a prosecution, if the proceedings for the prosecution have not been completed;

"PROCEEDING" means a court, civil or criminal proceeding or the hearing a matter over which an adjudicator is authorized under an Act of the Legislature or of Parliament to preside.

> **(1)(i)** a record made by or for a coroner that relates to an investigation, inquiry or inquest conducted by the coroner under the *Coroners Act* that has not been completed;

> **(1)(j)** a record of a service provider that does not relate to a service provided for or on behalf of a public body by the service provider;

This subsection clarifies that while a person working under contract for a public body is considered an **"EMPLOYEE"** of the public body, only the records that directly relate to that service may be accessed under this part of the *Act*. See **section 1** Definitions of the *Act* for more information.

> **(1)(k)** a record acquired by the archivist under section 9 of the *Archives Act* from a person other than a public body;

> **(1)(l)** personal health information held by a public body, or a program or activity of a public body, under its authority, and in relation to its function, as a custodian;

See Chapter 1, **Section 10** for more information on custodians.

> **(1)(m)** information contained in an examination or test;

> **(1)(n)** information contained in teaching materials;

> **(1)(o)** information gathered or created for the purpose of research conducted by

> **(1)(o)(i)** a researcher who is a member of the teaching faculty of Yukon University or another post-secondary institution,

(1)(o)(ii) a teaching or research assistant of a researcher referred to in subparagraph (i), or

(1)(o)(iii) any other person carrying out research in association with Yukon University or another post-secondary institution.

"YUKON UNIVERSITY" means the corporation continued as Yukon University under the Yukon University Act.

DIVISION 2 – OPEN ACCESS INFORMATION

SECTION 39 Information to be made available without access request

Application: Ministerial Public Bodies

This provision requires that certain types of information be proactively made available to the public, without the need for submitting an access request for these types of information. This provision applies only to **ministerial public bodies** and requires specific types of information to be disclosed by ministerial bodies, for example, the organizational structure, policies, manuals and final audit reports created and used by the public body.

This provision, in combination with **section 41**, requires the heads of ministerial bodies to proactively and on a recurrent basis, publish a list the types and classes of information that the ministerial body uses in providing services and carrying out programs or activities. The types of personal information collected can be included in this list (otherwise known as a "personal information banks" in other jurisdictions).

Subsection (a) requires the head of a ministerial public body to provide information on their structure, program, activity, and services to assist the public's ability to access information through the Open Access Registry and an access request under Division 3. This subsection will foster more transparency with the public by providing a greater understanding of government functions.

Providing the organizational structure may also assist Designated Access Officers when clarifying an access request with an applicant by identifying the division, unit, branch, etc. that is likely to hold responsive records the applicant is requesting.

"OPEN ACCESS INFORMATION" means the information and records described in paragraphs 39(a) to (d).

> **39** The head of a public body that is a ministerial body must make the following information and records available to the public in accordance with section 41:
>
> **39(a)** a description of each of the following with sufficient detail to facilitate the exercise of the right of access to information under this Act:
>
> **39(a)(i)** the public body's organizational structure, including, as applicable, each division, sub-division, unit, program or activity, or other type of component that forms a

part of its structure,

39(a)(ii) the public body's responsibilities and functions in respect of each of its organizational components, including the services of each component,

39(a)(iii) each current manual and policy statement that the head requires employees (other than service providers) of the public body to use or adhere to in carrying out a program or activity, or providing a service, of the public body,

39(a)(iv) each type or class of information and record described in accordance with section 40;

"PROGRAM OR ACTIVITY" of a public body, includes a service provided by the program or activity of the public body but does not include:

(a) a program or activity prescribed not to be considered a program or activity of the public body, or

(b) each of the following that is provided by the public body: (i) a specialized service, (ii) a data-linking activity, and (iii) an information management.

This definition provides that when this expression is used in this Act it is to include a service of a program or activity but not a program or activity that has been prescribed by Cabinet (under **subprovision 4(2)**) not to be a program or activity for the purpose of this Act, and also does not include specialized services (personal identity services and integrated services), data linking activities nor information management services.

The listed services and data-linking activities are scoped out of the expression because they are uniquely dealt under the Act compared to general programs and activities carried out by a public body. Each of these unique services or activity, before carried out by a public body, must obtain special Cabinet approval under **Part 2, Division 6**. This approval will set the parameters for the service or activity through the making of a regulation that specifies these parameters.

This expression is a key expression in respect of determining the scope and application the privacy provisions of this Act. However, the lack of a definition for this expression is intentional: no jurisdiction in Canada has substantively defined this expression but most use it. This expression is something of a relic from the original templates on which access and privacy legislation in Canada was based decades ago. It is also used (but not defined) in the previous Act to a limited extent. The expression is used much more frequently in the more modern access and privacy statutes enacted by other Canadian jurisdictions.

Legal research has identified the likely root of this expression being its use in financial administration legislation (this type of lexicon is currently used in the Financial Administration

Act (FAA), specifically at provision 21(1) of the FAA, which empowers Management Board to make a directive identifying “programs” and “distribute money among activities within a program”). Also, “programs” and “activities”, as concepts, are identified as distinct units of departments for the purpose of the government’s budget documents.

The Access and Privacy Officer is empowered under paragraph **86(1)(a)** with the power to issue protocols that will set out rules that provide guidance to public bodies in terms of the scope and description of a program or activity, or a service of program or activity. These protocols will reflect the laws and in the statute book (i.e. the FAA) and Cabinet direction on government organizational structure, and can be flexible over time if adjustments to government structure are made.

“PROTOCOL” means a protocol containing rules established by the Access and Privacy Officer under subsection 86(1).

For more on programs, activities and services, please see the General Overview in Chapter 2.

Subsection (b) encompasses the most common and requested types of information that the public may seek access to.

> **39(b)** a copy of each of the following that has been completed by or on behalf of the public body:
>
> **39(b)(i)** a public opinion poll or research study of public opinion,
>
> **39(b)(ii)** a statistical survey,
>
> **39(b)(iii)** an auditor’s final audit report,
>
> **39(b)(iv)** a final report, of a type other than an auditor’s final audit report, on the performance or efficiency of the public body, or the performance or efficiency of a program or activity, a specialized service or a data-linking activity of the public body,
>
> **39(b)(v)** a final report by a statutory body or any other body established (whether or not under an act) for the purpose of providing advice or recommendations to the public body in respect of a policy, program or activity, a specialized service or a data-linking activity of the public body,
>
> **39(b)(vi)** an appraisal report in relation to the value or condition of public property;

Subsection (c) is a discretionary provision that allows the head of a public body to make available information or a record available that is in the public interest.

> **39(c)** information or a record held by the public body for which the head is satisfied that it is in the public interest to make the information or record available to the public without requiring that an access request for the information or record be submitted;

Under **subsection (d)**, Cabinet can also prescribe types and classes of information that ministerial bodies will be required to make available to the public (i.e. the actual information, instead of strictly a list of information, will be required to be made openly accessible).

> **39(d)** information or a record of a type or class of information or record prescribed as open access information.

"PUBLICLY AVAILABLE INFORMATION" means personal information that is (a) contained in a public registry, (b) contained in a magazine, book, newspaper or other similar type of publication that is generally available to the public in print or electronic format, whether by purchase or otherwise, or (c) of a type or class of personal information prescribed as publicly available information.

"PUBLIC REGISTRY" means a registry (other than a court registry), register, roll, list or other thing that (a) is established or maintained under an Act, (b) contains personal information, and (c) is prescribed as a public registry.

SECTION 40 Types and classes of information and records used by public body

This provision requires that heads of ministerial bodies must establish at a *minimum of once a year*, update a list of the types and classes of information and records used by the ministerial body to carry out its programs, activities, and services. This list is to be made openly accessibly on an on-going basis in accordance with **section 39**.

This provision ensures the ministerial body is updating the type or class of information to reflect any changes in their organization.

> **40** For the purpose of subparagraph 39(a)(iv), the head of a public body that is a ministerial body must, periodically but not less frequently than once each year, describe each type or class of information or record that the public body uses in the course of carrying out each of its programs or activities or data-linking activities, or in the course of providing its specialized services.

For more on programs, activities, data-linking and specialized services, see **Chapter 2** of this manual.

SECTION 41 Making open access information available to public

This provision sets out how heads of ministerial bodies will make open access information available. Heads are required to create an 'open access registry' into which all open access information is required to be deposited.

"OPEN ACCESS REGISTER", of a public body, means the open access register established under paragraph 41(1)(a).

"OPEN ACCESS INFORMATION" means the information and records described in paragraphs 39(a) to (d).

It also requires **heads** to remove any information from open access records to which access is prohibited or denied in accordance with an exception to access under Part 3. It also states that the head is not required to deposit any open access information if it is in an incomplete or draft form or would be significantly redacted (under **section 43**).

For clarity, the public body may release the information with the same redactions it would apply, if the record were requested and released through an ATIPP request.

> **41(1)** The head of a public body that is a ministerial body must make open access information available to the public by
>
> **41(1)(a)** establishing an open access register for the public body;
>
> **41(1)(b)** subject to subsection (2), depositing all open access information into the open access register; and
>
> **41(1)(c)** maintaining the open access information deposited into the open access register in accordance with subsection (3).

Subsection 2 requires the head of a public body to ensure there is a process in place to review and sever any information to which a mandatory or discretionary exception to access may apply, before making it publically accessible in the Open Access Register.

> **41(2)** The head of a public body
>
> **41(2)(a)** must not deposit into the open access register the following information and records:
>
> **41(2)(a)(i)** generally excluded information,

41(2)(a)(ii) information or a record to which access is prohibited under Division 8; and

41(2)(b) may remove information from a record to be deposited into the register if the information is information to which the head may deny access under Division 9.

Subsection 3 provides the head of a public body with 90 days from the completion of a record under **section 39**, to upload it for public access into the Open Access Register.

41(3) The head of a public body must maintain open access information in a complete and accurate form by

41(3)(a) depositing it into the open access register not later than 90 days after the day on which the information is completed in its final form; and

41(3)(b) adding to, removing or changing any information or record contained in the open access register without delay after determining that it requires updating in order to be complete and accurate.

Subsection 4 provides exceptions to depositing information. This section clarifies that incomplete or draft records, information with a significant portion redacted using mandatory or discretionary exceptions and records over 15 years do not need to be uploaded into the Open Access Register.

41(4) The head of a public body is not required under this section to deposit into the public body's open access register

41(4)(a) information or a record that is incomplete or in a draft form; or

41(4)(b) despite paragraph 39(b)

41(4)(b)(i) a record for which access to a significant amount of information contained in the record is prohibited under Division 8 or to which the head may deny under Division 9, or

41(4)(b)(i) a record that has been in existence for 15 years or more.

SECTION 42 Fee for copy of open access information

This provision establishes that a fee may be charged for the making of a copy of open access information. Please see *ATIPP Act Regulation*.

> **42** If a fee is prescribed for the making of copies of records that have been deposited into a public body's open access register, a person who requests a copy of all or a part of a record must pay the prescribed fee in order to receive the copy.

SECTION 43 No limitation on release of information other than prohibited information

This provision clarifies that the head has discretion to make information available to an individual or the public except for information to which access is prohibited (e.g. cabinet information and confidential third party business information, for example).

This provision allows a head to provide any additional information not specified in the Act that may be of interest to the public, available without an access request.

> **43** For greater certainty, nothing in this Division is to be read as prohibiting the head of a public body from making any information or record, other than information or a record to which access is prohibited under Division 8, available to an individual or the public.

DIVISION 3 – REQUEST FOR ACCESS TO INFORMATION

SECTION 44 Right to request access to information

This provision allows an individual or a corporation (for profit and not for profit – a society) to submit an access request. There are no restrictions as to who may make a request. The applicant can be any person who is residing inside or outside of Yukon, including individuals, corporations, and organizations. The Act does not specify a minimum age, which means that minors may also make requests. An applicant means a person who makes a request for access to a record under **section 44.**

"ACCESS REQUEST" means a request submitted under subsection 44(1).

This section states that any person has the right to request access to any record held by a public body, including a record containing personal information about the applicant (**section 6(1)**). The type of information the individual can request is not constrained. If an applicant requests information that is generally excluded information under **section 38**, a response explaining the types of records and the provision for their exclusion must still be provided.

"HOLD", in respect of information, means to have custody or control of the information.

A public body has *custody* of a record, when the record is in the physical possession of the public body. A record is in the *possession* of a public body if the public body is physically holding or retaining the record. Some examples of records in the possession of a public body are: active records in an employee's office filing cabinet or in a central filing system on the public body's premises; inactive records in a records storage centre that may be located off the public body's premises; working papers in an employee's desk drawer and electronic records located on an employee's computer at work.

A record is under the control of a public body when the public body has the authority to manage the record, including restricting, regulating and administering it's use, disclosure of disposition.

Examples that a record may be in the custody or under the control of a public body are:

- The record was created by an officer, employee or member of the public body;
- The record was created by a service provider or information manager through a contract with the public body;
- The record is specified in a contract as being under the control of a public body;
- The record is in the possession of the public body;
- The record is closely integrated with other records of the public body;

- The content of the record relates to the public body's mandate and functions;
- The public body has the authority to regulate the record's use and disposition;
- The public body has relied upon the record to a substantial extent; or
- A contract permits the public body to inspect, review or copy records produced, retrieved, or acquired by a service provider.

The access request is submitted to the Access and Privacy Officer (ATIPP Office). The Access and Privacy Officer must make reasonable efforts to assist the individual making the request. The public body is similarly directed in section 64(5) to make reasonable efforts to respond to an applicant in an open, accurate and complete manner.

> **Section 44(1)** A person may request access to information (including their own personal information) held by a public body by submitting, in accordance with the regulations, if any, an access request to the access and privacy officer.

For more on submitting a request, see the *ATIPP Act Regulations*.

Subsection 2 provides the applicant with assistance with their request. This subsection establishes a duty of the Access and Privacy Officer (APO) or designate, to assist applicants in submitting their access requests. The APO or designate may request assistance from the public body to clarify or narrow a request. Applicants may submit the same access request to multiple public bodies. Each request is treated as a stand-alone, single request. Public bodies are not informed when the same request is submitted to multiple public bodies.

"APPLICANT", in respect of an access request, means the person who submits the access request.

This provision assists both the applicant and APO or designate, to **clarify the request**. Many applicants are unfamiliar with the organization and administrative practices of public bodies. They may not be aware of the process by which a public body reaches or implements a decision or policy, the kind of records that may be generated in the course of that process, and the process of disposing of the records.

The Access and Privacy Officer or designate may need to assist the applicant in clarifying the request so that the public body can retrieve records of interest to the applicant. Clarification of the request may involve assisting the applicant in defining the subject of the request, the specific kinds of records of interest, and the time period for which records are being requested. Narrowing a request as a result of the clarification process can have significant implications for fees.

> **44(2)** - The access and privacy officer must make reasonable efforts to assist an applicant in submitting an access request, including assisting the applicant in identifying in their submission under subsection (1) the public body that is to be the responsive public body in respect of the access request.

SECTION 45 Applicant information not to be disclosed

For most access to information requests it is unnecessary for the head to know the identity of the applicant. The application of the *ATIPP Act* does not change depending on who is requesting the information. Access to personal information requests are an exception, since the applicant must be identified in order for the public body to search for responsive records. It may also be necessary for the DAO to know the applicant in order to provide better service when processing the request.

This provision is designed to protect the identity of an applicant from the decision-maker. The Access and Privacy Officer (APO) or designate, is prohibited from disclosing the name of the applicant except in specific cases (i.e. with the designated access officer for the public body if the request is for personal information; personal information is required for the public body to respond; or the applicant consents to the disclosure).

> **45(1)** Subject to subsection (2), the access and privacy officer must not disclose to any other person
>
> **45(1)(a)** the name of the applicant; or
>
> **45(1)(b)** whether the applicant is an individual or a corporation.

Subsection 2 provides the Access and Privacy Officer with the discretion to release an applicants name for the purpose of responding to the request, or with the applicant's written consent.

> **45(2)** the access and privacy officer may disclose an applicant's name to
>
> **45(2)(a)** a designated access officer for the responsive public body if
>
> **45(2)(a)(i)** the access request is for the applicant's personal information,
>
> **45(2)(a)(ii)** the disclosure is necessary for the head of the responsive public body to respond to the access request, or
>
> **45(2)(a)(iii)** the applicant consents, in writing, to the disclosure; or

"RESPONSIVE PUBLIC BODY", in respect of an access request, means (a) if a copy of the access request has been provided to a head under subparagraph 47(2)(a)(i), the public body whose head has been provided the copy or, (b) otherwise, the public body whose head would be required to respond to the access request if it were to be accepted for processing under subsection 47(1).

Subsection (2)(b) provides the exception to confidentiality if the information is being disclosed to the Information and Privacy Commissioner (IPC) under a power or duty.

45(2)(b) the commissioner, if the commissioner has requested the disclosure for the purpose of their exercise of a power or performance of a duty under this Act.

"COMMISSIONER" means (a) the individual appointed as the commissioner under subsection 110(3), or (b) if no appointment has been made under subsection 110(3), the Ombudsman.

Examples:

PROGRAM REQUEST: Where the request is for general records, the ATIPP Office should forward only the request for records and not the name of the applicant or other identifiers to program areas within the public body. The APO may disclose the contact information to the DAO if it is necessary to process the request as the DAO may know more information about the file in order to respond in a more timely manner.

PERSONAL REQUEST: An access request contains recorded information about an identifiable individual. The personal information of the applicant can be disclosed to another employee of the public body only if the employee has a need to know that information in order to respond.

SECTION 46 Decision to accept or refuse access request

Under section **47(1)** of the Act, a request must provide enough detail to enable the public body to identify the record. The Access and Privacy Officer (APO) or designate has up to 10 business days after the day in which the request has been submitted, to assist the applicant and clarify the request before activating or refusing the request.

This provision requires the Access and Privacy Officer to make a decision, within 10 business days of the submission of an access request, on whether the request will be accepted or refused. This period (10 business days from the date of submission) are not included in the calculation of the day on which the head must respond to the access request (i.e. the response date as determined in accordance with section 50).

During this time period the APO or designate can work with the applicant and the public body to clarify the request. It is in the interest of both the applicant and the public body that the request is as precise as possible, since the applicant will receive the information they require with the minimum of work possible expended by the public body.

A public body should advise the APO or designate if a request does not sufficiently describe the records sought. The APO or designate should establish contact with the applicant to better understand what information will satisfy the applicant's needs. The public body should offer to the APO or their designate information relating to their records that will assist.

CLARIFYING REQUESTS

Vague or overly general requests may increase workloads and lead to review of information that is of little interest to the applicant and increase the costs to process the request. Often requests are broad or vague because the applicant lacks knowledge of the public body, its mandate and programs and the type of records available. (See Division 2 Open Access Information for information on the Open Access Register).

> **46(1)** Not later than 10 business days after the day on which an applicant submits an access request, the access and privacy officer must decide whether to
>
> **46(1)(a)** accept the access request for processing in accordance with section 47; or
>
> **46(1)(a)** refuse to process the access request in accordance with section 48.

Subsection 2 is the provision that provides the Access and Privacy Officer (APO) has deemed a request refused if they do not provide a response to the applicant before the end of the 10-day clarification period outlined in **section 44(2)**. This is a default clause providing in case notification does not occur. It allows the applicant to proceed with a complaint to the Information and Privacy Commissioner (IPC) under **section 49**. Section **47(2)(b)** requires the APO to provide a notice to the applicant that the request has been provided to the responsive public body for processing. **Section 48(3)** requires the APO to provide a notice to the applicant without delay that the request has been refused.

> **46(2)** If the access and privacy officer does not, before the end of the 10 business days referred to in subsection (1), take any action in respect of an access request, the access and privacy officer is considered to have decided to refuse the access request for processing on the day immediately following the 10th business day.

SECTION 47 Acceptance of access request

This provision requires the Access and Privacy Officer (APO) to accept a request for processing if there is sufficient detail included in the request and immediately provide a copy of the request to the responsive public body. The public body should acknowledge receipt of a request. The applicant will also receive notice that their request has been activated.

> **47(1)** The access and privacy officer must accept an access request for processing if they determine, in accordance with the regulations, if any, that the access request contains sufficient detail about the information being requested to reasonably enable the head of the responsive public body to respond to the access request.

Subsection 2 provides the process for notification to the head of the public body and applicant, once the request has been accepted. The applicant's identity is not provided to the public body as part of the request *unless it is needed* to process the request (i.e. personal information request or APO determines it is necessary) or the applicant has consented as per **section 45**.

> **47(2)** Without delay after accepting an access request for processing, the access and privacy officer must provide
>
> **47(2)(a)** subject to section 45, a copy of the access request to
>
> **47(2)(a)(i)** the head of the responsive public body, and
>
> **47(2)(a)(ii)** a designated access officer for the responsive public body; and
>
> **47(2)(b)** a notice to the applicant that states that their access request has been provided to the responsive public body for processing.

"ACTIVATION DATE", in respect of an access request, means the day on which the access and privacy officer provides a copy of the access request to the head of the responsive public body under subparagraph 47(2)(a)(i).

SECTION 48 Refusal of access request

This provision sets out the criteria for the Access and Privacy Officer (APO) to refuse to process an access request.

> **48(1)** Subject to subsection (2), the access and privacy officer may decide to refuse to process an access request if

Subsection (1)(a) empowers the Access and Privacy Officer to refuse a request if there is not sufficient detail for the public body to respond. Note that under **section 44(2)**, the APO has a duty to assist an applicant throughout the process of submitting a request.

> **48(1)(a)** they determine under subsection 47(1) that the access request does not contain sufficient detail about the information being requested to reasonably enable the head of the responsive public body to respond to the access request; or

Subsection (1)(b) provides the basis for the Access and Privacy Officer to make a determination to refuse to process an access request.

> **48(1)(b)** they determine, in accordance with the regulations, if any, that

Subsection (1)(b)(i) empowers the Access and Privacy Officer to refuse a request if it is substantially similar to information that was already provided to the applicant by the same public body.

> **48(1)(b)(i)** the access request is for access to substantially the same information that the head of the responsive public body provided to the applicant in response to an access request previously submitted by the applicant,

Subsection (1)(b)(ii) empowers the Access and Privacy Officer to refuse a request if it is substantially similar to a request made by the applicant within the previous 60 days for which the head of the public body already responded to.

> **48(1)(b)(ii)** the access request is for access to substantially the same information that the applicant requested from the head of the responsive public body in an access request submitted by the applicant within the 60-day period preceding the day on which the access request was submitted, or

Subsection (1)(b)(iii) empowers the Access and Privacy Officer to refuse a request if a significant amount of 'research and compilation' would be required to process the request to such an extent that the processing of the request would unreasonably interfere with the operations of the public body.

In order to make a claim for UNREASONABLE INTERFERENCE, the responsive public body must provide evidence that responding to the request would obstruct, or hinder the range of effectiveness of the body's activities. Public bodies should allocate a sufficient amount of resources to respond to access requests and must provide sufficient evidence beyond "time and effort" to support a claim or unreasonable interference. To read more on interference, see **section 62**.

> **48(1)(b)(iii)** based on the amount of information that could reasonably be identified as relevant to the access request, the amount of research, compilation and examination of information that would be required to be undertaken by the responsive public body would unreasonably interfere with the responsive public body's operations.

RESEARCH means finding the information and COMPILING means bringing it together.

For example, the threshold to refuse a request based on unreasonable interference would be extremely high. An applicant is required to pay for requests that meet criteria defined in the *ATIPP Act Regulations* **section 54** and a public body can request an extension for this reason under **section 52(2)(a)**.

Subsection 2 mandates that consultation with the applicant and public body occurs *before* the Access and Privacy Officer (APO) can refuse a request. Only if the consultation is not successful, can the APO consider refusing the request.

Section 46(1) requires the Access and Privacy Officer to make a decision, within 10 business days of the submission of an access request, whether the request will be accepted or refused.

During this time period the APO or designate, can work with the applicant and the public body to clarify the request. It is in the interest of both the applicant and the public body that the request is as precise as possible, since the applicant will receive the information they require with the minimum of work and cost possible expended by the public body.

A public body should advise the Access and Privacy Officer or designate if a request does not sufficiently describe the records sought. The APO or designate should establish contact with the applicant to better understand what information will satisfy the applicant's needs. The public body should offer to the APO or their designate information relating to their records that will assist.

CLARIFYING REQUESTS: Vague or overly general requests may increase workloads and lead to review of information that is of little interest to the applicant. Often requests are broad or vague because the applicant lacks knowledge of the public body, its mandate and programs and the type of records available. (See **Division 2** Open Access Information of this Chapter for information on the Open Access Register).

> **48(2)** Before deciding to refuse to process an access request, the access and privacy officer must consult with
>
> **48(2)(a)** the applicant who submitted the access request; and
>
> **48(2)(b)** the head of the responsive public body.

Subsection 3 outlines the process for notification to both parties once a decision to refuse access has been made. If the notification does not occur within 10 business days after receipt, the request is deemed refused under section 46(2).

> **48(3)** Without delay after deciding to refuse to process an access request, the access and privacy officer must provide a notice of the decision to the applicant that includes
>
> **48(3)(a)** the reasons for the decision; and
>
> **48(3)(b)** a statement notifying the applicant of their right to make a complaint under section 49.

SECTION 49 Complaint in respect of refusal of access request

This provision establishes an applicant's right to complain to the Information and Privacy Commissioner about the decision to refuse their request, if they are unsatisfied with the response or disagree with the refusal.

> **49** An applicant may, in respect of a decision to refuse to process their access request, make a complaint to the commissioner by filing the complaint in accordance with section 90.

For more on the complaint process, see **section 90** in Chapter 5.

PART 3

DIVISION 4 – PROCESSING OF ACCESS REQUEST

SECTION 50 Response date for access request

This provision requires the head to respond to an access request in **30 business days** from the activation date (e.g. the date on which the Access and Privacy Officer (APO) decides to accept the access request for processing.

"RESPONSE DATE", in respect of an access request, means the date determined under section 50 by which the head of a responsive public body must respond to the access request.

This provision clarifies that this period is suspended during the time in which the applicant has the right to make a decision if provided with a cost estimate, to either pay the costs of the access request, or apply and are granted a waiver of the cost. If the applicant does not make this decision within *20 business days* after being provided the cost estimate, the Access and Privacy Officer may determine their access request to be abandoned under **section 58**.

Subsection 1 outlines the head's responsibility for responding to a request within 30 business days, or in the date determined under an extension. Heads may request more than one extension.

The head of a public body is required to respond to an access request within 30 business days from the activation date *unless* an extension of the response date is granted. The activation date is the day after the date on which the APO decides to accept the access request for processing and sends a copy of the request to the public body under **section 47(1)(a)**. If an extension is granted, the timeline for the response will change. A notice will be provided to the applicant with the new response date for them to receive a response to their access request.

> **50(1)** Subject to subsection (2), the head of a responsive public body must respond to an access request in accordance with section 64 not later than
>
> **50(1)(a)** the 30th business day following the activation date for the access request; or
>
> **50(1)(b)** if one or more extensions are granted under subsection 62(2) or subparagraph 63(2)(a)(i) in respect of the access request, the latest response date provided under the extensions.

Subsection 2 provides for a hold on the access request to allow for the applicant to make a decision on costs if provided with an estimate under **section 54**. Applicants may:

- choose to pay,

- work with the Access and Privacy Officer to narrow the scope to reduce costs,
- apply for a waiver of part or all costs,
- withdraw the request, or
- not respond and have the request eventually declared abandoned.

50(2) The period described in subsection (3) is not to be included in the calculation of the response date for an access request under subsection (1).

Subsection 3 outlines that the hold begins on the date when the applicant is provided with an estimate of cost and ends on the date the applicant is either provided with a notice of the Access and Privacy Officer's decision to grant the applicant a waiver, or on the date the applicant agrees to pay all or a portion of the prescribed costs.

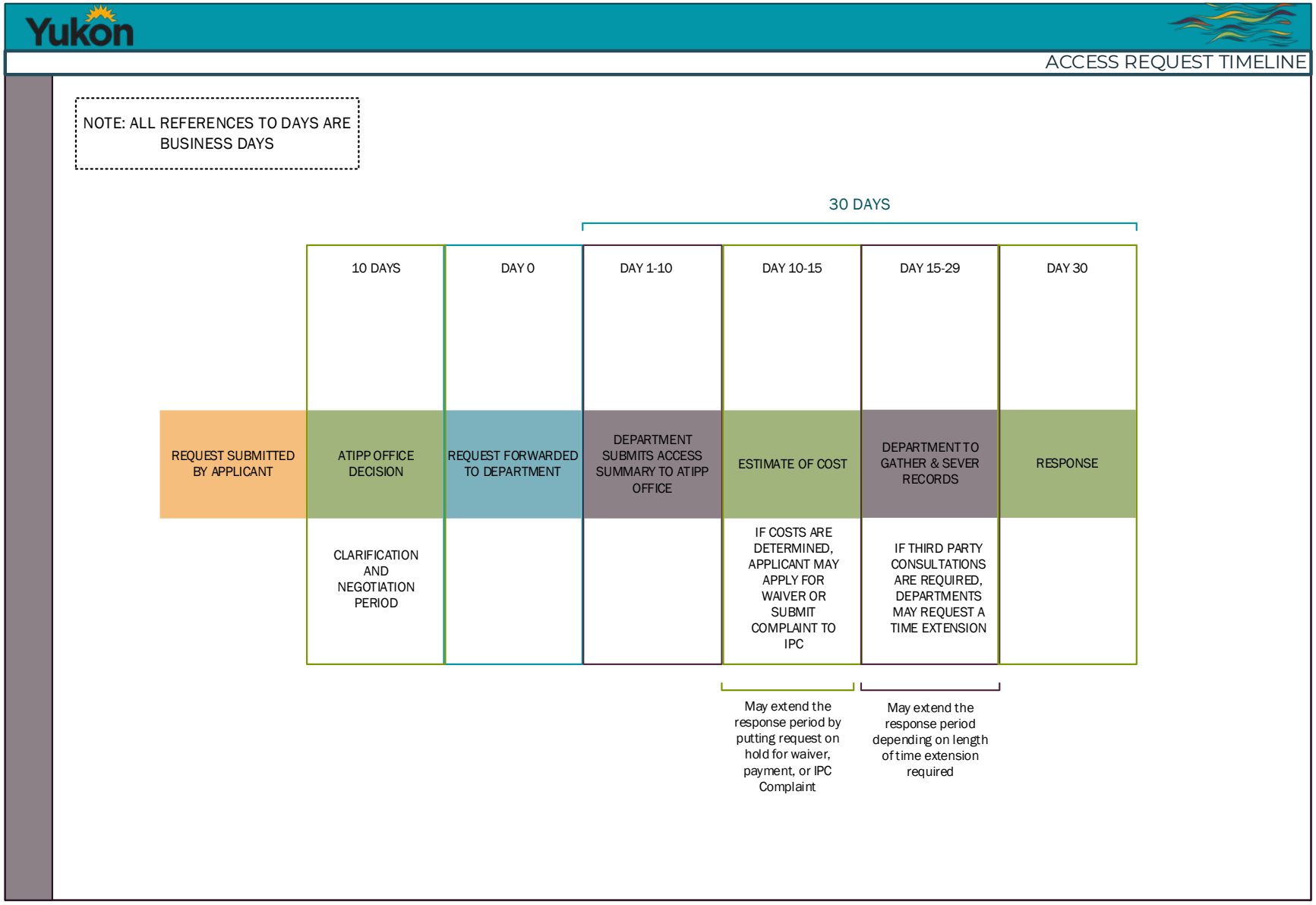
50(3) The period referred to in subsection (2) is the period that begins on the day on which the applicant is provided with a cost estimate for their access request in accordance with paragraph 54(2)(b) and ends on, as applicable

50(3)(a) the day on which the applicant is provided with a notice of a decision to grant the applicant a waiver of costs in respect of their access request under paragraph 56(1)(b); or

50(3)(b) otherwise, the day on which the applicant agrees to pay the prescribed cost, or a portion of the prescribed costs, for processing their access request in accordance with paragraph 55(1)(a).

For more on extensions, see Division 6 of this Chapter.

FIGURE 6.1 – Access Timelines



SECTION 51 Request for relevant information

This provision requires the Designated Access Officer (DAO) to request information relevant to the access request from employees within the public body who the DAO reasonably believes hold such information. The same request may be made to the head if the DAO believes that they also hold relevant information. The DAO determines the date on which employees must respond.

"DESIGNATED ACCESS OFFICER", of a public body, means an employee designated under paragraph 87(1)(b) as a designated access officer for the public body.

> **51** Without delay after receiving a copy of an access request under subparagraph 47(2)(a)(ii), the designated access officer who received the copy must
>
> **51(a)** make a request, in accordance with the regulations, if any, for all information relevant to the access request
>
> **51(a)(i)** to the head of the responsive public body, if the designated access officer reasonably believes the head is likely to hold information relevant to the access request, and
>
> **51(a)(ii)** to each employee of the responsive public body who the designated access officer reasonably believes is likely to hold information relevant to the access request; and
>
> **51(b)** specify the date by which the head's, and each employee's, response to the request must be provided to the designated access officer.

TIMELINES

The Designated Access Officer (DAO) must provide the Access and Privacy Officer (APO) or designate with the **Access Information Summary** within **10 business days** of receiving the activated request in accordance with **section 53**. This may mean the public body employees have a very limited time frame to conduct the search (3-5 business days).

The Designated Access Officer (DAO) will decide on the date the employee response is due in order to meet the 10 day Access Information Summary deadline. The employee is obligated under **section 52(1)** to provide the DAO with a response *by that date*. If the employee does not provide a response by the date, the DAO must note this in the Access Information Summary provided to the Access and Privacy Officer and report the lack of response to the Head of the Public Body as outlined in **section 52(2)(b)**.

SEARCH

Details of a request should be forwarded to any program area that may hold the requested records with a due date for employees to respond. A search for responsive records must consider all records, as defined in the *Act*, including all electronic records, hard copy etc. that are held (in the custody or under the control) of the public body. A public body must search all locations, including individual offices, central active files and off-site locations, where records may be found.

The search for electronic record may include electronic information management systems, business applications, shared directories, e-mail systems, websites, collaboration sites, and social media. Electronic devices, including laptops, tablets, SmartPhones and other personal mobile devices, cellular phones, portable media and storage devices, may need to be searched as well. Hardcopy includes any paper documentation, letters, files etc.

A public body may also have to search for responsive records under its control that are in the hands of a third party, who is contracted as a **"SERVICE PROVIDER"**. Under this *Act*, service providers are considered to be employees.

"SERVICE PROVIDER", of a public body, means a person who, under contractor, provides a service for or on behalf of the public body and includes an employee or agent or the service provider.

However, **section 38(1)(j)**, generally excluded information, includes that "a record of a service provider that does not relate to a service provided for or on behalf of a public body by the service provider", is not to be considered held by the public body. This limits how far a public body can reach into a service provider's records.

A public body's records and information management staff may be able to identify finding aids that will assist in locating relevant records in paper and electronic formats.

A public body must be prepared to support claims for the ADEQUACY OF SEARCH with evidence as to how the public body conducted its search in the particular circumstances. The search strategy, not the amount of time spent on a search, will determine whether a public body has conducted an adequate search.

A public body is not required to search electronic back-up, as this is generally excluded information under **section 38(2)**.

A public body cannot decide not to conduct a search for records on the basis of an opinion that no responsive records exist. In a case where a public body has conducted a previous search in response to another request, if there is any doubt that the request is for substantially the same information, the public body *must conduct a completely new search*. If the other search was substantially similar but earlier, the public body must search for records that may have been created since the earlier request.

Other Public Bodies

A public body is not required to search for records held by other public bodies.

In the event that a public body employee is aware of another public body that may hold records requested under an access request, they should inform the Designated Access Officer, who in turn will contact the ATIPP Office as soon as possible to allow them to notify the applicant.

The applicant may agree to withdraw the request and submit a new access request to the other public body for records. However, unless the request is withdrawn, the original request and search must continue until the public body can reasonably prove there are no records found.

SECTION 52 Duty to respond to designated access officer

This provision establishes a duty on employees to respond to a request for relevant information by providing the Designated Access Officer (DAO) with an estimate of the amount of information they hold by the date specified by the DAO.

"EMPLOYEE", of a public body, includes (a) an individual who is:

(i) an employee of the public body, or of another public body that provides a service to the public body, appointed to a position in the public service pursuant to the *Public Service Act*,
(ii) a principal, vice-principal or teacher, or technical support staff, of the public body appointed to their position pursuant to the Education Act, or
(ii) an employee appointed to a position pursuant to the *Cabinet and Caucus Employees Act* for the purpose of assisting the minister responsible for the public body,
(b) a service provider of the public body,
(c) a director, or officer of the public body, or
(d) any other individual who provides a service to the public body, whether or not for compensation.

Section 52 of the Act stipulates that the employee and the head of a public body have a duty to provide the Designated Access Officer (DAO) with all of the accurate and responsive information that pertains to any access request that they receive. The DAO is also responsible for notifying the head if an employee does not respond to a request within the assigned timeline. The lack of response is also noted in the Access Information Summary provided by the DAO to the Access and Privacy Officer (APO).

This section holds all parties accountable with a duty to assist.

52(1) The head and each employee of a responsive public body who receive a request under paragraph 51(a) must, by the date specified in the request, provide a response to the designated access officer who made the request

52(1)(a) indicating whether they hold information relevant to the access request; and

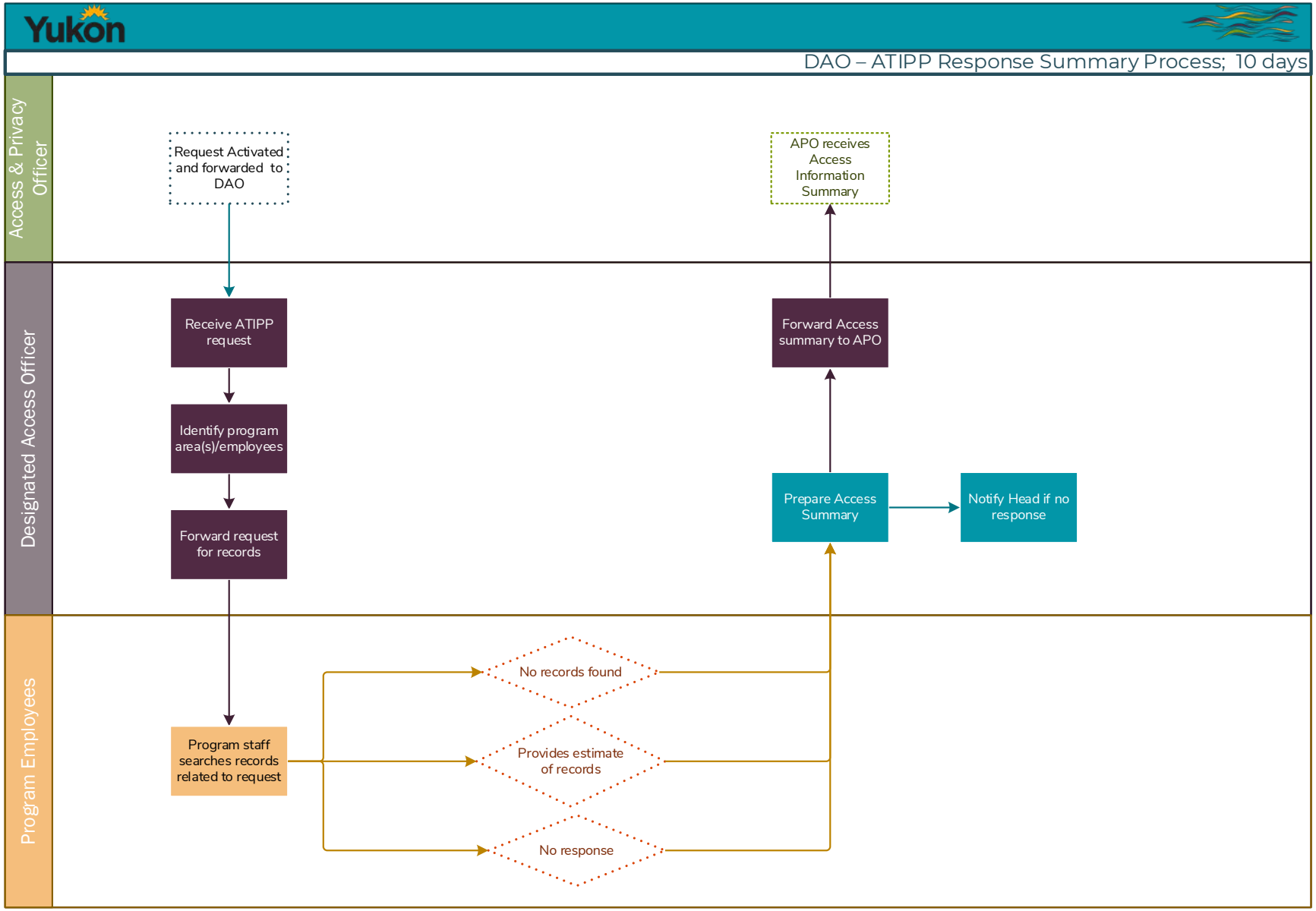
52(1)(b) if they hold information relevant to the access request

52(2) If an employee who is required to provide a response under subsection (1) does not respond to the request by the date specified in the request, the designated access officer must

52(2)(a) make a note in the access information summary for the access request to which the request relates indicating that the employee did not respond to the request; and

52(2)(b) without delay, report the lack of response to the head of the responsive public body.

FIGURE 6.2 ACCESS INFORMATION SUMMARY TIMELINE FOR PUBLIC BODY



SECTION 53 Access information summary

This provision requires the Designated Access Officer (DAO) to compile an "Access Information Summary" within 10 business days of the first day on which processing of the access request starts. The DAO must then provide it to the Access and Privacy Officer (APO). The summary will include the amount of information located in each program or activity. It will be used by the APO to determine the cost estimate for processing the request as outlined in **section 54**.

"ACCESS INFORMATION SUMMARY", in respect of an access request, means the written summary provided to the Access and Privacy Officer under section 53 for the access request.

> **53** Not later than 10 business days after the activation date for an access request, the designated access officer must, in accordance with the regulations, if any, provide to the access and privacy officer a written summary of the responses provided to them under subsection 52(1) in respect of their request for all information relevant to the access request that
>
> **53(a)** sets out the estimated amount of information relevant to the access request; and
>
> **53(b)** specifies each program or activity of the responsive public body that holds information relevant to the access request.

SECTION 54 Cost estimate determination

This provision requires the Access and Privacy Officer (APO) to determine the cost estimate (if any) to process an access request within the specified timeframe – not later than 5 business days after the day on which an "Access Information Summary" was provided. In making the determination, the APO will use the formula established in *ATIPP Act Regulations*.

> **54(1)** Not later than five business days after the day on which an access information summary is provided under section 53, the access and privacy officer must determine, in accordance with the regulations, the cost estimate for processing the access request.

Subsection 2 instructs the Access and Privacy Officer to either notify the public body to continue with the access request if there will be no costs charged, or provide an estimate of cost to the applicant if costs will be charged. The public body should not proceed with a request after producing an Access Information Summary until they receive notification from the APO (ATIPP Office).

> **54(2)** Immediately after making a determination of the cost estimate for processing an access request under subsection (1), the access and privacy officer must

> **54(2)(a)** if the cost estimate is zero, notify, without delay, a designated access officer for the responsive public body to proceed with processing the access request; and
>
> **54(2)(b)** if the cost estimate is more than zero, provide a copy of the cost estimate and the access information summary for the access request to the applicant.

Subsection 3 establishes that if the Access and Privacy Officer does not provide the applicant with an estimate of cost within the 5 business days required under **section 54(1)**, that no costs can be charged to the applicant and the public body must proceed with processing the request.

This section encourages the public body and Access and Privacy Officer to provide information for determining costs in a timely manner or they will lose an important tool to assist with narrowing the scope of a request.

> **54(3)** If the access and privacy officer does not, before the end of the five business days referred to in subsection (1), provide the cost estimate for the processing of an access request, and the access information summary, to the applicant under paragraph (2)(b)
> **54(3)(a)** the cost estimate for processing the access request is considered to be zero; and
>
> **54(3)(b)** the access and privacy officer must, without delay, provide notification to a designated access officer under paragraph (2)(a).

Subsection 4 establishes an applicant's right to complain to the Information and Privacy Commissioner (IPC) if the applicant does not agree with the cost estimate.

If the applicant makes a complaint to the Commissioner under subsection (3), time is suspended while the Commissioner processes the complaint in respect of a determination under **section 58** that the access request is abandoned.

> **54(4)** An applicant to whom a copy of a cost estimate is provided under paragraph (2)(b) may make a complaint to the commissioner by filing the complaint in accordance with section 90.
>
> **54(5)** Subsection 58(1) does not apply to an access request in respect of which a complaint has been filed in accordance with subsection (4) during the period that begins on the day on which the complaint is filed and ends on, as applicable
>
> **54(5)(a)** the day on which the commissioner dismisses the complaint under subparagraph 91(1)(a)(ii); or
>
> **54(5)(b)** the day on which the respondent provides a notice to the complainant under subparagraph 104(1)(b)(i) in respect of the complaint.

SECTION 55 Applicant's decision to pay prescribed cost

This provision provides the applicant with the right to make a choice in respect of how to proceed with their access request, once they are provided with the cost estimate.

Applicants can:

- agree to pay the cost for processing the request
- agree to pay a portion of the cost, by clarifying their request
- apply for a full or partial waiver of costs

If the applicant agrees to pay for a portion of the cost, then the remaining portion of the access request is considered abandoned.

If the applicant does not make a decision and take action under this provision within 20 business days of receiving the cost estimate, the Access and Privacy Officer may, under **section 58**, determine the access request to be abandoned.

The time for processing the request by the public body is suspended while the applicant decides to either agree to pay the fees or apply for a waiver (this is set out in **section 50** in respect of the calculation of the response date for an access request).

If the applicant makes a complaint to the Information and Privacy Commissioner regarding the estimate of cost under **subsection 54(3)**, time is suspended while the Commissioner processes the complaint in respect of a determination under **section 58** that the access request is abandoned.

> **55(1)** On receiving the cost estimate for processing their access request under paragraph 54(2)(b), an applicant may, in accordance with the regulations
>
> **55(1)(a)** agree to pay
>
> **55(1)(a)(i)** the prescribed cost for processing the access request, or
>
> **55(1)(a)(ii)** subject to subsection (2), if the applicant requests that only a portion of their access request be processed, the prescribed cost for processing that portion of the access request; or
>
> **55(1)(b)** apply for a waiver of the requirement to pay the prescribed cost, or a portion of the prescribed cost, for processing the access request.

55(2) If an applicant agrees to pay the prescribed cost for processing only a portion of their access request under subparagraph (1)(a)(ii)

55(2)(a) the access request is considered to be only that portion of the applicant's original access request; and

55(2)(b) the remaining portion of the access request is, for the purposes of this Act, considered to be abandoned.

SECTION 56 Decision – waiver of prescribed cost

This provision requires the Access and Privacy Officer to decide in 10 business days whether to grant a waiver of cost, or a portion of the cost, for the processing of an access request if an applicant applies for a waiver and to notify the applicant of the decision. For more information, see the *ATIPP Act Regulations*.

56(1) Not later than 10 business days after the day on which an applicant applies for a waiver, the access and privacy officer must, in accordance with the regulations, if any

56(1)(a) decide whether to

56(1)(a)(i) grant to the applicant a waiver of the requirement to pay the prescribed cost, or a portion of the prescribed cost, or

56(1)(a)(ii) refuse to grant to the applicant a waiver of the requirement to pay the prescribed cost, or a portion of the prescribed cost; and

56(1)(b) provide a notice of the decision to the applicant.

Subsection 2 outlines what happens in the case that the Access and Privacy Officer does not provide the notification outlined in subsection(1)(b). In this instance the waiver is considered to have been refused.

56(2) If the access and privacy officer does not, before the end of the 10 business days referred to in subsection (1), provide a notice of decision to the applicant in accordance with paragraph (1)(b), the applicant's application for the waiver to which the notice relates is considered to have been refused by the access and privacy officer under subparagraph (1)(a)(ii) on the day immediately following the 10th business day.

Subsection 3 allows for an applicant to complain to the commission if their waiver is refused

56(3) An applicant whose application for a waiver is refused may make a complaint to the commissioner by filing the complaint in accordance with section 90.

Subsection 4 establishes an applicant's right to complain to the Commissioner if the applicant does not agree decision to refuse a waiver. If the applicant makes a complaint to the Commissioner under subsection (3), time is suspended while the Commissioner processes the complaint in respect of a determination under **section 58** that the access request is abandoned.

56(4) Subsection 58(1) does not apply to an access request in respect of which a complaint has been filed in accordance with subsection (3) during the period that begins on the day on which the complaint is filed and ends on, as applicable

56(4)(a) the day on which the commissioner dismisses the complaint under subparagraph 91(1)(a)(ii); or

56(4)(b) the day on which the respondent provides a notice under subparagraph 104(1)(b)(i) in respect of the complaint to the complainant.

SECTION 57 Notice to proceed with processing access request

This provision requires the Access and Privacy Officer to notify the Designated Access Officer to proceed with processing the request *after* the applicant agrees to pay the cost of processing the access request. A public body should not proceed before receiving this notice.

57(1) The access and privacy officer must provide notice to a designated access officer for the responsive public body to proceed with processing the access request

57(1)(a) without delay after the applicant agrees to pay, in accordance with paragraph 55(1)(a), the prescribed cost, or a portion of the prescribed cost, for processing the access request; or

57(1)(b) on granting a waiver to the applicant under subparagraph 56(1)(a)(i).

57(2) Without delay after being provided with notice under subsection (1) to proceed with processing an access request, the designated access officer who receives the notice must proceed with processing the access request.

SECTION 58 Abandonment if no action taken by applicant

This provision enables the Access and Privacy Officer to declare the request abandoned if the applicant does not respond to the cost estimate provided after 20 business days.

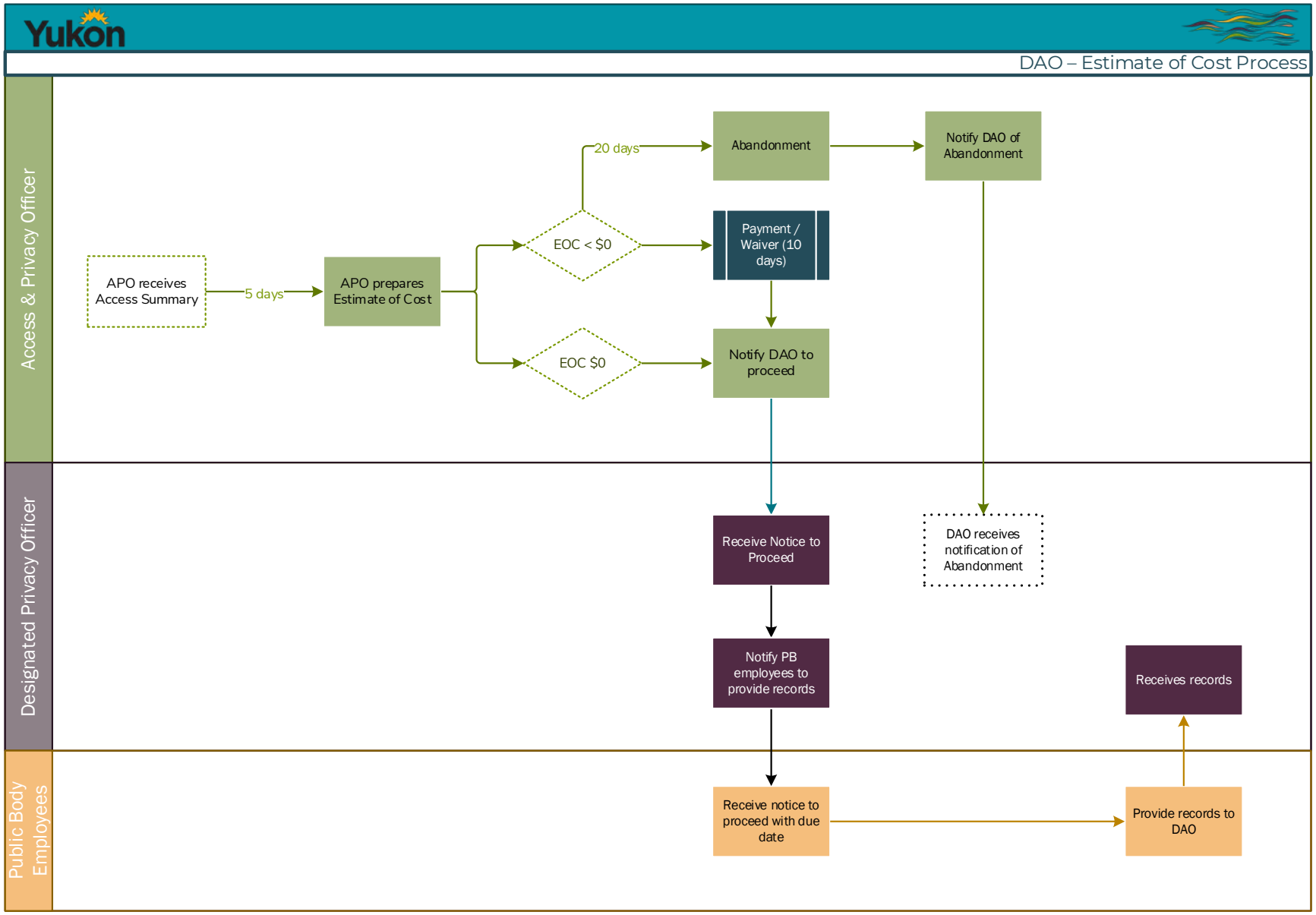
> **58(1)** If, on the 20th business day following the day on which a cost estimate is provided to an applicant under paragraph 54(2)(b), the applicant has not agreed to pay the prescribed cost for processing their access request in accordance with paragraph 55(1)(a) or has not been granted a waiver under subparagraph 56(1)(a)(i) in respect of their access request to which the cost estimate relates, the access and privacy officer may
>
> **58(1)(a)** determine that the access request is abandoned;
>
> **58(1)(b)** take no further action in respect of the access request; and
>
> **58(1)(c)** if the access and privacy officer makes a determination under paragraph (a), provide without delay after making the determination, a notice to the applicant that their access request has been determined abandoned.

Subsection 2 establishes the right of an applicant to make a complaint to the Commissioner if their access request has been determined to be abandoned under sub provision (1).

> **58(2)** An applicant to whom a notice is provided under paragraph (1)(c) may make a complaint to the commissioner by filing the complaint in accordance with section 90.

For more on complaints, see **section 90** in Chapter 5.

FIGURE 7.1 ESTIMATE OF COST PROCESS



PART 3

DIVISION 5 – THIRD PARTY NOTICE

SECTION 59 Seeking third party's view on granting access

This provision establishes the process for consulting with a third party in the event a head is considering granting access to the third party's personal information or non-confidential business information. The decision whether to consult with a third party in this case, is at the **discretion** of the head (e.g. it is not mandatory).

NOTE: This section cannot be used for information accepted in confidence in the manner prescribed through the *ATIPP Act Regulations*.

The head may notify the third party and provide them with the opportunity to provide reasons why the information should not be released or give their consent to release the information.

"THIRD PARTY" means a person other than the applicant or the responsive public body. A third party may be a person, a group of persons, or an organization other than an applicant or a public body. Third parties also include individuals, sole proprietorships, partnerships, corporations, unincorporated associations and organizations, non-profit groups, trade unions, syndicates and trusts. An employee of a public body can also be a third party.

PUBLIC BODIES are ministerial bodies and any other statutory body or entity that is prescribed in the regulations. Please see *ATIPP Act Regulations* for more information. Governments that are not public bodies, (federal, provincial, municipal, First Nation) are considered to be third parties if the release of personal or non-confidential business information is involved. Informal consultation with other governments not pertaining to this type of information does not follow this process.

A public body should consult with a third party if it intends to release information that may harm the third party. For example, if a public body has decided that disclosure of third party business information could reasonably be expected to cause significant harm to the third party's competitive position, the third party may be able to provide information supporting a decision on non-disclosure.

A public body may also choose to consult a third party to request consent to release information that would normally not be disclosed. For example, a third party may agree to have their personal information released to an applicant as part of a statement involving the applicant.

Subsection 1 requires the head of the public body to provide a notice to the applicant, third party and Access and Privacy Officer that a third party consultation is being sought. This consultation may affect the responsive date for the access request if an extension is granted under **section 62(1)(vi)**.

> **59(1)** The head of a responsive public body may, before responding under section 64 to an access request that could grant access to a third party's personal information or a third party's non-confidential business information as described in subsection 77(1), seek the third party's view on the matter, by
>
> **59(1)(a)** providing the following notices:
>
> **59(1)(a)(i)** a notice to the third party in accordance with subsection (2),
>
> **59(1)(a)(ii)** a notice to the applicant in accordance with subsection (3); and
>
> **59(1)(b)** providing a copy of each notice referred to in paragraph (a) to the access and privacy officer.

Subsection 2 outlines the requirements of a notice to a third party. The notice must follow the requirements on the information they may be considering releasing and to request their comments on the release on a specific date.

> **59(2)** The notice provided to a third party under subparagraph (1)(a)(i) must
>
> **59(2)(a)** state
>
> **59(2)(a)(i)** that the that the third party's information has been identified as information relevant to an access request, and
>
> **59(2)(a)(ii)** that the head of the responsive public body is considering whether to grant access to the information;
>
> **59(2)(b)** specify
>
> **59(2)(b)(i)** the response date for the access request, and
>
> **59(2)(b)(ii)** the date by which the third party may submit written objections to the head in respect of granting access to the information; and
>
> **59(2)(c)** include a copy of the information, or if not practicable to do so, a description of it.

If a record that is the subject of a third party notice contains information that is not the third party's, the public body may redact this information from the record sent to the third party for consultation. If the record sent for consultation contains personal information which is not the third party's the information must be redacted to prevent a privacy breach. If the personal information cannot be redacted it may be best to simply describe the record in the notice.

The head of the public body is responsible for setting the due date for the third party to respond to the consultation. In setting the due date the head should consider that if the public body decides to release information that the third party has objected to the release of under **section 60(2)**, notice must be provided to the third party and the applicant 10 business days before the response date for the access request. This time period is provided to give the third party the opportunity to make a complaint to the Commissioner.

The public body can request a time extension from the Access and Privacy Officer under **section 62(v)**, if additional time is needed for the consultation.

Subsection 3 outlines the requirements of a notice to the applicant. The notice must inform the applicant that information relevant to a third party is part of the response and that the third party is being provided an opportunity to submit objections to its release.

> **59(3)** The notice to an applicant under subparagraph (1)(a)(ii) must state that
>
> **59(3)(a)** a third party's information has been identified as information relevant to the applicant's access request; and
>
> **59(3)(b)** the third party is being provided an opportunity to submit written objections in respect of granting access to the information.

SECTION 60 Notice of decision to grant access

If the head decides to release third party information despite the third party's objections, the head is required to notify the third party of the decision at least 10 days before the head must respond to the access request to which they are considering granting access to the third party's information. The content of the notice will vary according to circumstances.

A public body must decide whether to withhold or grant access to third party information on the basis of factors relevant to the applicability of **section 59.** However, the public body can consider comments or statements from a third party that may be relevant to other exceptions, when it is considering whether any other exceptions apply to the record.

Subsection 1 outlines the public body's responsibility to inform the third party and the applicant of a decision to release information where a third party has objected to its release.

> **60(1)** If, by the date on which written objections may be submitted to the head of a responsive public body in accordance with a notice provided to a third party under subparagraph 59(1)(a)(i), the third party submits objections to the head and, despite the objections, the head decides to grant access to the third party's information, the head must provide a notice of the decision to
>
> **60(1)(a)** the applicant to whom the decision relates; and
>
> **60(1)(b)** the third party.

The public body only needs to provide notice to the third party and applicant if the decision is to release and the applicant has objected in writing.

Subsection 2 specifies that the notice of decision to release must be sent to the third party and applicant at least 10 business days before the response date for the request.

> **60(2)** The notice under subsection (1) must be provided not later than 10 business days before the response date for the access request to which the notice relates.

To reduce the need for review of decisions by the Commissioner, public bodies should provide applicants and third parties with clear explanations of their decisions, the provision(s) of the *Act* that apply and the reasons why they are applicable in the particular instance. These explanations provide a basis for discussion of the decision and may help the public body and the applicant to settle any outstanding issues without recourse to the Office of the Information and Privacy Commissioner (OIPC).

SECTION 61 Complaint – notice to grant access to third party information

This provision establishes a third party's right to complain to the Information and Privacy Commissioner (IPC) in the case where the third party received notice from a head that they have decided to grant access to the third party's information. The third party must make this complaint at least 5 days before the response date for the access request and if it is made, time is suspended only in respect of the head's response regarding that information. For more information, see **Chapter 5** – Commissioner's investigations for more information.

> **61** Not later than five business days before the response date for an access request in respect of which a notice has been provided to a third party under paragraph 60(1)(b), the third party may, in respect of the head of the responsive public body's intention to grant access to the third party's information, make a complaint to the commissioner by filing the complaint in accordance with section 90.

When a complaint is made to the Commissioner the public body does not provide the response to the applicant until the investigative report on notice of dismissal is received from the commissioner. After receiving the report or notification the public body has 5 business days to provide the response under **section 92**.

During an investigation by the Commissioner under **section 102(b)** the burden of proof rest with the third party to explain why granting access to this information would be harmful to them.

DIVISION 6 – EXTENSION OF TIME FOR RESPONSE

SECTION 62 Limited extension by Access and Privacy Officer

This provision allows the head of a public body to ask the Access and Privacy Officer (APO) to extend the time limit for responding to a request in accordance with section 62(2) without seeking the permission of the Information and Privacy Commissioner (IPC).

There are a number of reasons as to why a public body may need more time to process an access request and this section covers those reasons. For instance, this may occur if a consult with a third party is not recognized until late in the processing of a large request. In this case, the extension is needed to provide sufficient time to comply with the notification provisions of the Act.

If the request is incomplete and further information is required from the applicant in order to identify the records sought, a public body should seek this information immediately. The requirement to clarify the request does not change the date on which the time period commences, but may necessitate a time limit extension. Ideally the clarification would be completed during the clarification/negotiation stage with the APO before the access request is activated.

A public body may request an extension from the Access and Privacy Officer within the time limits under section 62**.** The Access and Privacy Officer may extend the time limit to a maximum of 15 business days without the applicant's written permission, or 30 business days with the applicant's written permission.

> **62(1)** Not later than five business days before the response date for an access request, the head of a responsive public body may make a written request (with reasons) to the access and privacy officer for an extension of the time within which the head must respond to the access request.

The APO will not accept extension requests that are submitted later than 5 days before the response date. It's important for public bodies to understand the timelines and their requirements for extension requests. Failure to provide a response on the due date will result in the head being considered to have denied the applicant access to all the relevant information and may trigger a complaint to the IPC.

The public body must make the extension request in writing and support the request with reasons. A detailed explanation identifying the reasons for the request assist the Access and Privacy Officer in evaluating the extension request. The APO must determine where necessary

if the reasons provided meets the test of **unreasonably interfering** with the responsive body's operations. This determination is based on the amount of information identified in the Access Information Summary and whether multiple requests have been submitted. The APO may choose to share the detailed reasons supporting the extension provided by the public body with the applicant when a notice is provided as per section 62(4).

Unreasonable interference may vary between public bodies. When requesting an extension where the APO is directed to consider unreasonable interference as a factor, the public body must provide evidence that responding to the request would obstruct, or hinder the range of effectiveness of the body's activities. Public bodies should allocate a sufficient amount of resources to respond to access requests and must provide sufficient evidence beyond "time and effort" to support a claim of unreasonable interference.

The following is a list of examples that may be considered to unreasonably interfere with the responsive body's operations.

Circumstances that may contribute to unreasonable interference:

- Significant increase in ATIPP requests (e.g. sharp rise over 1-4 months)
- Computer systems or technical problems
- Unexpected analyst leave (analyst on file)
- Unusual number (high percentage) of analysts-in training
- Program area discovers a significant amount of additional records
- Type of records (maps, etc.)
- Number of program areas searched
- Location of records
- The number and size of requests closed since the request was received
- Whether the current load of requests is higher than a public body's two-year average

Invalid Circumstances:

- The operation has not been allocated sufficient resources
- Long term or systemic problem(s)
- Vacations
- Office processes (e.g. sign-off)
- Personal commitments
- Pre-planned events (e.g. retirements)
- Previous extensions taken and no work done on file
- Number of requests closed is below the two-year average

Subsection 2 outlines the reasons for which the Access and Privacy Officer can grant an extension. This provision states the extension must be granted not later than the third business day after receiving the request for an extension from the public body. These reasons include:

volume and complexity of the request, receiving multiple concurrent requests form one applicant or entity, the public body requiring additional information or the public body requiring time for consultations.

> **62(2)** Not later than the third business day after receiving a request under subsection (1), the access and privacy officer may, subject to subsection (3), grant the extension if
>
> **62(2)(a)** the access and privacy officer determines that
>
> **62(2)(a)(i)** based on the amount of information identified as relevant to the access request, the amount of research, compilation and examination of information that would be required to be undertaken by the responsive public body to enable the head to respond to the access request by the response date would unreasonably interfere with the responsive public body's operations,

Subsection (2)(a)(i) details the information the Access and Privacy Officer may weigh in evaluating if the request will unreasonably interfere with the operations of the public body. This includes the volume (page count) of material that must be searched and or reviewed, the accessibility of the information and unusual circumstances surrounding the processing of the information. For example, does the type of the record require different methods of searching or handling? Is outside assistance required to access the files?

> **62(2)(a)(ii)** because of multiple concurrent access requests submitted by the applicant to the responsive public body, requiring the head to respond to the access request by the response date would unreasonably interfere with the responsive public body's operations,

Subsection (2)(a)(ii) details the information the Access and Privacy Officer may weigh in evaluating if the request will unreasonably interfere with the operations of the public body. These include the number of concurrent requests from the same applicant and the public body's timeline for addressing each individual one.

> **62(2)(a)(iii)** because of multiple concurrent access requests submitted by the applicant and at least one other applicant on behalf of, or in association with, the same entity or each other to which the head of the responsive public body is required to respond, requiring the head to respond to the access request by the response date would unreasonably interfere with the responsive public body's operations,

Subsection (2)(a)(iii) details the information the Access and Privacy Officer may weigh in evaluating unreasonable interference including the number of concurrent requests from the same entity and the public body's timeline for addressing each individual one.

> **62(2)(a)(iv)** the responsive public body reasonably requires more information from the applicant to process the access request,

Subsection (2)(a)(iv) details the information the Access and Privacy Officer may weigh in evaluating the request, includes the importance of the information to the processing of the request and the circumstances why this information is needed at this stage as opposed to the clarification/negotiation period before the request was accepted.

> **62(2)(a)(v)** the responsive public body reasonably requires more time to
>
> **62(2)(a)(v)(A)** consult with another public body whose information has been identified as relevant to the access request and is held by the responsive public body, or

Subsection (2)(a)(v)(A) details the information the Access and Privacy Officer may weigh in evaluating the request, including the number, volume and complexity of the needed consults. Details may include: when the public body initiated consultations, large number of consultations, availability of third parties being consulted and deadlines provided. Extensions should not normally be needed for routine, small, inter-department consults.

> **62(2)(a)(v)(B)** consult with a person, government or other entity (other than a public body) that the head reasonably believes is likely to be adversely affected by granting access to information identified as relevant to the access request, or

Subsection (2)(a)(v)(B) details the information Access and Privacy Officer may weigh in evaluating the request, including the number, volume and complexity of the consultations.

> **62(2)(a)(vi)** the head reasonably requires more time to seek the views of a third party whose information has been identified as relevant to the access request; or

Subsection (2)(a)(vi) details the information the Access and Privacy Officer may weigh in evaluating the request, including the number, volume and complexity of the needed consults and whether the consults are occurring as per **section 59** as they relate to third party personal or non-confidential business information.

Subsection (2)(b) allows for the applicant to provide written consent for the extension.

> **62(2)(b)** the applicant consents, in writing, to the extension.

If the applicant consents in writing to the extension, the Access and Privacy Officer may grant an extension of up to 30 business days in accordance with **section 62(3)(a)**.

Subsection 3 states that the Access and Privacy Officer can grant multiple extensions. The total time period of these extensions cannot exceed **15 business days** unless the applicant has

agreed in writing. If the applicant agrees in writing, the total time period of extensions cannot exceed **30 business days**.

> **62(3)** The access and privacy officer may grant more than one extension in respect of an access request but the total number of business days in respect of all extensions granted for the access request must not exceed
>
> **62(3)(a)** if the applicant consents in accordance with paragraph (2)(b), 30 business days; or
>
> **62(3)(b)** otherwise, 15 business days.

Subsection 4 requires the Access and Privacy Officer to notify the applicant and the head of the granted time extension, with the reasons for granting the extension and the new responsive date for the access request.

> **62(4)** Without delay after the access and privacy officer grants an extension under subsection (2), they must provide a notice to the applicant and the head who requested the extension that
>
> **62(4)(a)** states that an extension has been granted and the reasons for granting the extension; and
>
> **62(4)(b)** specifies the new response date for the access request.

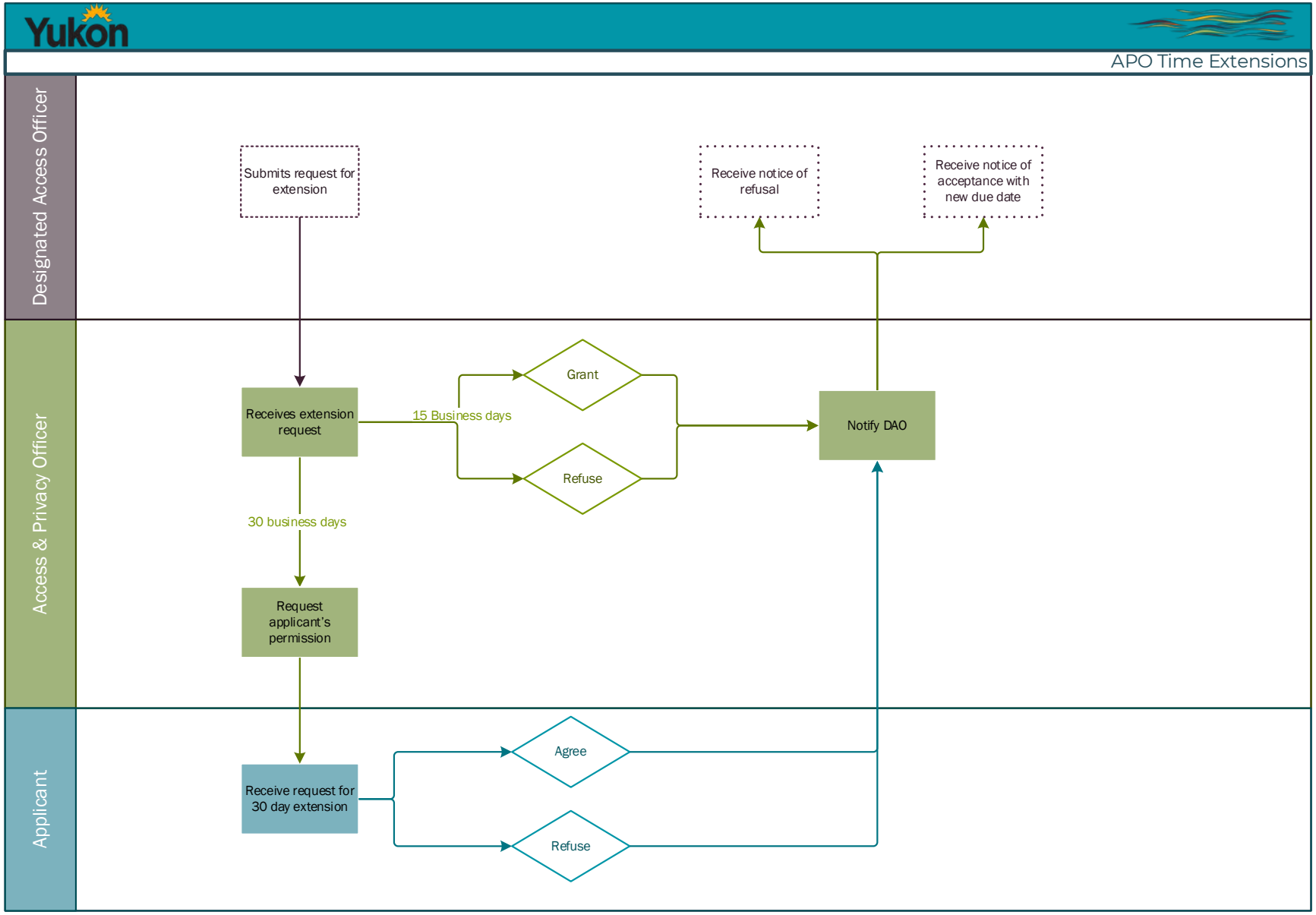
The Access and Privacy Officer may choose to share the detailed reasons supporting the extension that were provided by the public body in the extension request, with the applicant.

Subsection 5 establishes the right of an applicant to complain about the extension to the Information and Privacy Commissioner.

> **62(5)** An applicant to whom a notice is provided under subsection (4) may make a complaint to the commissioner by filing the complaint in accordance with section 90.

Possible complaints may include the time period of the extension or the validity of the reasons for granting the extension.

FIGURE 8.1 TIME EXTENSION - DESIGNATED ACCESS OFFICER



SECTION 63 Unlimited extension by commissioner

In this provision, if a public body believes that it still cannot complete processing of the request within the extension period provided by the Access and Privacy Officer (APO) under **section 62**, the public body may ask the Information Privacy Commissioner (IPC) for a longer extension not later than **8 business days** before the response date for an access request. There is no maximum time limit on this extension period, and is solely on the discretion of the IPC.

Subsection 1 establishes the time frame for a public body to seek an extension request from the Commissioner to 8 business days before the response date for an access request. Public bodies should continue to process a request while awaiting the Commissioner's response to an extension request.

> **63(1)** Not later than eight business days before the response date for an access request, the head of a responsive public body may make a written request (with reasons) to the commissioner for an extension of the time within which the head must respond to the access request.

Subsection 2 provides the responsibility of the Commissioner for providing notice of their decision and reasons to the head and applicant within 3 business days. If an extension is granted the notice includes the new response date.

> **63(2)** Not later than the third business day after receiving a request under subsection (1), the commissioner must
>
> **63(2)(a)** subject to subsection (3), decide whether to
>
> **63(2)(a)(i)** grant an extension, or
>
> **63(2)(a)(i)** refuse to grant an extension; and
>
> **63(2)(b)** provide a notice to the applicant and the head who requested the extension that
>
> **63(2)(b)(i)** states their decision with reasons, and
>
> **63(2)(b)(ii)** if an extension is granted, specifies the new response date for the access request.

Subsection 3 highlights the requirements for the Commissioner to use the determination set out in **subsections 62(2)(a)(i)-(v)** in making the determination to grant or refuse the extension request: unreasonable interference with the operations of a public body due to the amount of

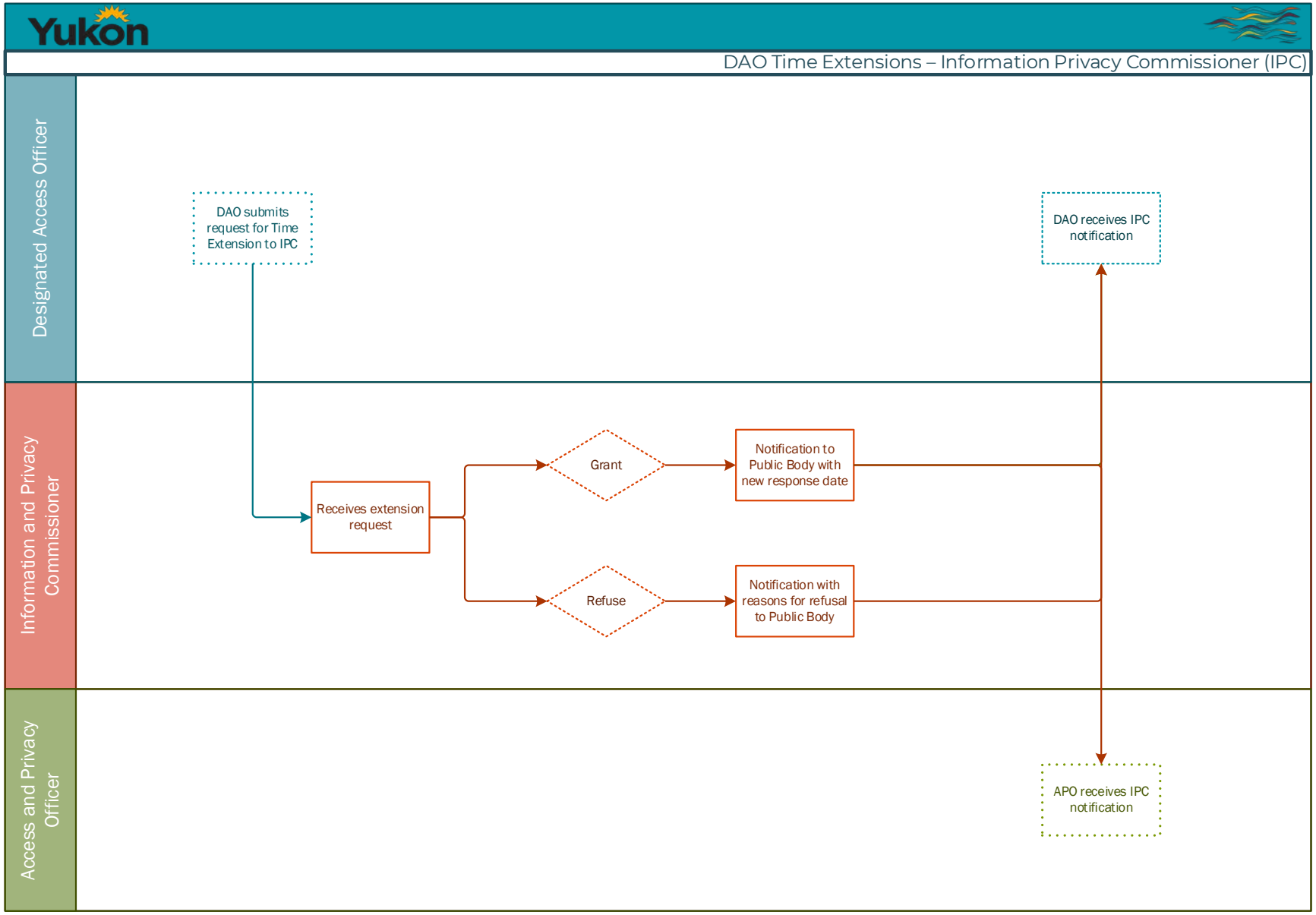
information, or multiple concurrent requests by the same or multiple applicants or due to the need for additional information or consultations with third parties.

> **63(3)** In deciding whether to grant or refuse to grant an extension under subsection (2), the commissioner must
>
> **63(3)(a)** consider whether any of the circumstances referred to in subparagraphs 62(2)(a)(i) to (vi) apply to the request for the extension; and
>
> **63(3)(a)** if any of those circumstances apply, consider that circumstance a sufficient ground for granting the extension.

Subsection 4 clarifies that the Commissioner's decision is not limited only to the requirements of **subsections 62(2)(a)(i)-(v)** unreasonable interference with the operations of a public body due to the amount of information, or multiple concurrent requests by the same or multiple applicants or due to the need for additional information or consultations with third parties.

> **63(4)** For greater certainty, nothing in subsection (3) limits the commissioner's discretion to grant an extension on grounds other than the grounds referred to in that subsection.

FIGURE 8.2 TIME EXTENSION - INFORMATION AND PRIVACY COMMISSIONER



PART 3

DIVISION 7 – RESPONSE TO ACCESS REQUEST

SECTION 64 Response to Access Request

This provision states that the head of a public body must make every reasonable effort to assist applicants to respond to each applicant openly, accurately and completely.

The head of the responsive public body must respond to an access request, whether the public body holds responsive records or does not. Requests cannot be ignored if the Designated Access Officer (DAO) is advised by employees that they do not hold records.

Subsection 1 requires the head to respond by the response date and provides the contents of the response, including granting access to all relevant information held by the public body with exceptions to access narrowly applied.

> **64(1)** Subject to subsections (3) and 92(1), the head of the responsive public body must respond to an access request, through the access and privacy officer or in the prescribed manner, if any, not later than the response date for the access request, by
>
> **64(1)(a)** granting the applicant access to all the information relevant to the access request that is held by the responsive public body except the information and records withheld under paragraph (b);
>
> **64(1)(b)** withholding from the applicant, in accordance with the regulations, if any, the following information and records relevant to the access request that are held by the responsive public body:

Subsection (1)(b)(i) requires the withholding of Generally excluded information (see section 38(1)(a) to (o)).

> **64(1)(b)(i)** information and records that the head has determined are generally excluded information,

Subsection (1)(b)(ii) requires the withholding of information to which access is prohibited. See mandatory exemptions beginning part 3.

> **64(1)(b)(ii)** information and records to which the head has determined that access is prohibited under Division 8,

Subsection (1)(b)(iii) allows for the withholding of information to which access may be denied. See discretionary exemptions in the Overview at the beginning of this Chapter.

> **64(1)(b)(iii)** information and records to which the head has decided to deny the applicant access under Division 9;

Subsection (1)(c) requires a public body to provide access by copying or allowing the applicant to examine records if they cannot be copied in accordance with section 65 Provision of access.

> **64(1)(c)** subject to paragraph (7)(b), providing the applicant with access to the information to which they have been granted access in accordance with section 65, and
>
> **64(1)(d)** providing the applicant with written reasons for the response in accordance with subsection (2).

Under **subsection (1)(d)** the head must provide reasons in accordance with subsection (2), which includes specifying the provision of this Part on which the head has relied for the purpose of withholding information and providing any further explanation that is necessary.

Subsection 2 specifies what information needs to be included in the head's written response to an applicant:

- The head must specify provision(s) providing authority to provide access to information or deny access to information – the head may also provide any additional rationale on why they decided to withhold the information that could help the applicant understand why the information was withheld;
- The head must include the business contact information of the employee of the responsible public body for whom the applicant may contact;
- The head must include a notice of the applicant's right to complain to the Information and Privacy Commissioner about the head's response.

> **64(2)** The head's written reasons for their response to an access request must
>
> **64(2)(a)** in respect of each determination or decision made under paragraph (1)(b)
>
> **64(2)(a)(i)** specify the provision of this Part under which the determination or decision was made, and
>
> **64(2)(a)(ii)** in the case of a decision referred to in subparagraph (1)(b)(iii), provide any further explanation that the head considers necessary to substantiate their reason for making the decision;

64(2)(b) include the business contact information of the employee of the responsive public body whom the applicant may contact in respect of a question relating to the head's response to the access request; and

64(2)(c) include a notification to the applicant of their right to make a complaint under section 66 in respect of the response.

Subsection 3 authorizes the head to not reveal the existence of information or a record. Such a decision is limited to information that may cause harm to an individual, is related to law enforcement information or could threaten public health or safety.

64(3) The head of a responsive public body may decide not to reveal in their response, in accordance with subsection (4), the existence of information or a record relevant to an access request only if

64(3)(a) the information is, or the record contains, personal information for which the head has determined that revealing its existence to the applicant could reasonably be expected to cause significant harm to an individual; or

"SIGNIFICANT HARM" means in respect of paragraph 64(3)(a), bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property, or any other similar types of harm.

64(3)(b) the information or record is of a type or class of information or record to which the head may deny access under subsection 72(1) or section 79.

Subsection 64(4) requires the head to notify the commissioner of the reasons why the decision was made to not reveal the existence of information or record. This requirement ensures proper oversight of a head's decision to use this provision.

64(4) If the head of a responsive public body decides not to reveal the existence of information or a record under subsection (3), the head must

64(4)(a) in respect of their response to the applicant, state that no information or record was identified in respect of the matter to which the information or record relates; and

64(4)(b) without delay after making the decision, provide the commissioner with a notice of their decision, including the reasons for the decision.

Subsection 5 places a duty on the head to assist an applicant to receive the information they are seeking.

> **64(5)** The head of a responsive public body must make reasonable efforts to respond to an applicant under this section in an open, accurate and complete manner.

Subsection 6 requires the head to notify the IPC of their denial of access, if they do not respond by the response date.

> **64(6)** If the head of a responsive public body does not respond to an access request by its response date
>
> **64(6)(a)** the head is considered to have denied the applicant access to all the information relevant to the access request that is held by the responsive public body; and

If the head does not provide a response by the response date, the applicant can complain to the Information and Privacy Commissioner under section 66 that access has been denied. The public body should still provide a late response to the applicant if access has been denied under this provision.

> **64(6)(b)** the head must, without delay after the response date, provide to the commissioner a notice that no response was provided by the response date and that states the reason why a response was not provided.

Subsection 7 clarifies that the head of the public body must provide a response by the access request response date to the Access and Privacy Officer, but must not provide access to the records until the applicant pays the prescribed cost, if any.

> **64(7)** If, by the response date for an access request, the applicant has not paid the prescribed cost for processing the access request that they agreed to pay under paragraph 55(1)(a), the head of the responsive public body
>
> **64(7)(a)** is still required to respond to the access request (through the access and privacy officer or in the prescribed manner, if any) by its response date; and
>
> **64(7)(b)** must not, until the applicant has paid the prescribed cost, provide the applicant with access in accordance with section 65 to the information to which they have been granted access.

Subsection 8 authorizes if the prescribed cost for access is not provided by the applicant on the 31 business day, the request is declared abandoned and the file is closed.

> **64(8)** If, by the 31st business day following the response date for an access request, the applicant has not paid the prescribed cost for processing the access request, the head of the responsive public body must consider the access request abandoned.

SECTION 65 Provision of Access

Section 65 sets out how the head of a responsive public body must provide an applicant access to the information or records to which the applicant has been granted.

Subsection (1)(a) is a provision that sets out how the head of a responsive public body has an obligation to, provide access to the all the relevant information made in an access request as referred to in **section 64**. The access to the information should be in the form of a copy of the requested information so long as a copy of the information could be reasonably produced.

In the case where a copy of a record cannot be reasonably produced and provided to the applicant, the head is required to provide an opportunity for the applicant to examine the information contained in the record.

> **65(1)** The head of a responsive public body must, in accordance with the regulations, if any, provide an applicant with access to the information referred to in paragraph 64(1)(a) by
>
> **65(1)(a)** in the case of information of which the responsive public body can reasonably make a copy, providing the copy of the information to the applicant; or
>
> **65(1)(b)** in the case of information of which the responsive public body cannot reasonably make a copy, providing the applicant with a reasonable opportunity to examine the information.

The provision described in **subsection 2** requires the head to provide information that was contained in an electronic medium if it is reasonable to do so and the technical capacities exist to produce it.

It is only considered reasonable, if the request would not interfere with the regular operations of the applicable public body.

> **65(2)** If information to which an applicant has been granted access is contained in an electronic medium, the head of the responsive public body must provide a copy of the information to the applicant only if
>
> **65(2)(a)** the copy can be created using the technical capabilities of the responsive public body; and
>
> **65(2)(b)** the head is satisfied that providing the copy would not unreasonably interfere with the operations of the responsive public body.

Subsection 3 requires the head to provide the electronic information in a re-useable manner if the technical capacities exist to produce it and it would not unreasonably interfere with the regular operations of the public body. The example of this is an applicant puts in a request for

information to be provided in a specific file type such as excel, or a dataset which would allow the applicant to be able to edit and manipulate the data at a later date.

"DATASET" means a grouping of data in which all or most of the data (a) is held by a public body, (b) consists of facts, (c) is not the product of analysis or interpretation, (d) is not a document referred to in section 9 of the *Archives Act*, and (e) has not, except for its grouping, been organized, adapted or modified.

> **65(3)** If information to which an applicant has been granted access is contained in an electronic medium and is, or forms part of, a dataset, the head of the responsive public body must provide a copy of the information to the applicant in an electronic form that is capable of re-use only if
>
> **65(3)(a)** the information can be provided in that form using the technical capabilities of the responsive public body; and
>
> **65(3)(b)** the head is satisfied that providing the information in that form would not unreasonably interfere with the operations of the responsive public body.

Subsection 4 provides discretion for the head to create a record where reasonable to do so and the applicant has requested it. An example of this would be when an applicant is more interested in the summary of the information contained in the records then being provided with all the original records.

> **65(4)** The head of a responsive public body may create a record that contains information in a medium other than the medium in which the responsive body ordinarily holds the information if
>
> **65(4)(a)** the applicant has requested the information in the other medium; and
>
> **65(4)(b)** the applicant has requested the information in the other medium would be less costly for the responsive public body than providing it in the original medium.

If the public body determines that it would be more cost effective to generate a record containing the requested information than providing the record, the applicant must agree to receive the information in this format.

Subsection 5 provides that a head is not required to translate a document into a language requested by the applicant. This means that the language in which the record is kept is the one the applicant will receive.

> **64(5)** This provision provides that a head is not required to translate a document into a language requested by the applicant.

SECTION 66 Complaint – response to access request

This provision states that if an applicant is not satisfied with the response of a public body, they can submit a complaint to the Information and Privacy Commissioner (IPC).

> **66** An applicant may, in respect of the head of a responsive public body's response to their access request under section 64, make a complaint to the commissioner by filing the complaint in accordance with section 90.

The Commissioner has the authority to review the process and application of the *ATIPP Act* that the public body used to formulate their response. If in their review, the Commissioner finds that something was not done properly or according to the *Act* they can facilitate the release of further or withheld information from that public body.

Alternatively, they may find that the public body has conducted its search properly and has followed the *Act* correctly.

PART 3

D8

DIVISION 8 – INFORMATION TO WHICH ACCESS IS PROHIBITED

SECTION 67 Cabinet Information

This provision deals with information that is considered under the definition of a Cabinet Record and looks at what information can be released under this term and what cannot be released.

"CABINET" means the Executive Council and includes a committee of the Executive Council.

In **Subsection 1,** the definition of **"CABINET RECORD"** clarifies which records are subject to this exception.

> **67(1)** In this section "Cabinet record" means, subject to subsection (2)
>
> **67(1)(a)** A record containing advice or recommendations prepared for or submitted to Cabinet,
>
> **67(1)(b)** A draft bill or regulation prepared for or submitted to Cabinet,
>
> **67(1)(c)** A record containing briefing material prepared for or submitted to Cabinet,
>
> **67(1)(d)** An agenda for a Cabinet meeting, or a minute or other record of the deliberations or a decision of Cabinet,
>
> **67(1)(e)** A record that reflects communications or discussions among ministers in respect of the making of a government decision or the formulation of government policy,

Subsection (1)(e) is intended to capture information in records that may not have been included in the definition of a "Cabinet record". For example, emails discussing matters that relate to assessing a course of Cabinet action.

> **67(1)(f)** A record created for a minister for the purpose of briefing the minister on a matter that is before, or is to be brought before Cabinet
>
> **67(1)(g)** A record created for the purpose of a submission to Cabinet, or
>
> **67(1)(h)** A part of a record that contains information about the contents of a record of a type referred to in paragraphs (a)-(g)

Subsection 2 carves out certain types of information that, if included in a Cabinet record that are not to be considered a part of the Cabinet record (i.e. the exception under this provision does not apply to this information). Other parts of the *Act* may apply to the decision to release or withhold this information.

> **67(2)** For the purpose of the definition "Cabinet record" in subsection (1), information of the following types is not considered to be a Cabinet record or a part of a Cabinet record:
>
> **67(2)(a)** factual information included in a Cabinet record only for the purpose of providing contextual background information;
>
> **67(2)(b)** information included in a Cabinet record for the purpose of providing Cabinet with a background explanation or analysis for its consideration in making a decision but only if
>
> **67(2)(b)(i)** the decision has been made public,
>
> **67(2)(b)(ii)** the decision has been implemented, or
>
> **67(2)(b)(iii)** five years or more have passed since the decision was made or the matter was considered by Cabinet;
>
> **67(2)(c)** information in a Cabinet record that reflects the decision of Cabinet in respect of an appeal brought before it under an Act.

Subsection 3 establishes the exception to access to Cabinet records and information revealing the substance of Cabinet deliberations. It requires the head to refuse access to an entire record if it is a cabinet record, or if information in the record is not a cabinet record as per subsection 2 the parts of the record that is a cabinet record. Access to information in a record other than a Cabinet record is also prohibited if the information would reveal the substance of the deliberations of Cabinet. However, if either of these (Cabinet record or the information) has been in existence for 10 years or more, this exception does not apply to the record or information. Other parts of the *Act* may apply to the decision to release or withhold this information.

> **67(3)** Except if a Cabinet record or information has been in existence for 10 years or more, the head of a responsive public body must not grant an applicant access to any of the following held by the responsive public body:
>
> **67(3)(a)** a Cabinet record;

> **67(3)(b)** information contained in a record other than a Cabinet record that, if disclosed, would reveal the substance of the deliberations of Cabinet.

Subsection 4 provides for a specific public interest override to the exception under sub provision (3) that may be exercised by the Secretary of the Executive Council by considering the public interest in transparency over the public interest in withholding the information.

> **67(4)** The Secretary of the Executive Council may grant an applicant access to information contained in a Cabinet record or information referred to in paragraph (3)(b) if they determine that the public interest in disclosing the Cabinet record or information clearly outweighs the public interest in maintaining the Cabinet record or information as a Cabinet confidence.

SECRETARY OF THE EXECUTIVE COUNCIL means the member of the public service appointed under the *Government Organisation Act* as the Secretary of the Executive Council.

SECTION 68 Confidential information from another government

This provision states that a public body can refuse to disclose information that has been accepted in confidence in the prescribed manner. *ATIPP Act Regulations* will specify the manner in which information must be accepted by a public body for it to be considered confidential information under this provision.

This provision does not overlap with section 76 Disclosure harmful to intergovernmental relations. Only one section may be applied, not both.

ACCEPTED IN CONFIDENCE only applies when the public body follows the prescribed manner in which to accept information as set out in the *ATIPP Act Regulations*.

This provision only applies to ATIPP requests. If a Public Body accepts information in confidence, it is not released if found responsive to an access request. It is the public body's responsibility to ensure that confidential information is properly maintained outside of the ATIPP process, or risk its release in another manner.

Information that does not meet the threshold for being accepted in confidence can rely on other provisions under this Act that relate to harm, including **section 76** Disclosure harmful to intergovernmental relations.

Subsection 1 specifies the government bodies external to the Government of Yukon, to certain First Nation governments and to local government bodies.

The exception also covers any of their agencies (i.e. corporate bodies or persons designated by any of the listed external government organizations). For example, the Department of National

Defence is an agency of the Government of Canada, UNESCO is an agency of the United Nations, and an economic development agency is an agency of a local government. The provision covers not only *provincial governments* but also t*erritorial governments* and their agencies.

> **68(1)** Subject to subsections (2) and (3), the head of a responsive public body must not grant an applicant access to information held by the responsive public body that a public body has, in the prescribed manner, accepted in confidence from
>
> **68(1)(a)** the Government of Canada;
>
> **68(1)(b)** the government of
>
> **68(1)(b)(i)** a province, or
>
> **68(1)(b)(ii)** a foreign state;
>
> **68(1)(c)** a First Nation government;

"FIRST NATION GOVERNMENT" means (a) a governing body established under the constitution of a Yukon First Nation, (b) the council of a band recognized under the Indian Act (Canada), or (c) an entity prescribed as a First Nation government.

> **68(1)(d)** a municipality;

"MUNICIPALITY" means a municipality established under the *Municipal Act* and includes (a) the corporation established under that Act for the municipality, and (b) the council of the municipality.

> **68(1)(e)**an organization representing one or more governments; or
>
> **68(1)(f)**an international organization of states.

Subsection 2 allows the head to grant access to information to which this exception applies if the information has been in existence for more than 15 years, or if the other government consents to the granting of access or has made the information available to the public. This is discretionary whereas, **section 76** Disclosure harmful to intergovernmental relations, is a mandatory release of the information.

> **68(2)** The head of a responsive public body may grant an applicant access to information referred to in subsection (1) if
>
> **68(2)(a)** the information has been in existence for 15 years or more; or
>
> **68(2)(b)** the government or organization from which the information was accepted
>
> **68(2)(b)(i)** consents, in writing, to the disclosure of the information, or

> **68(2)(b)(ii)** has made the information available to the public.

The Public Body can review the decision to hold accepted information in confidence and release this information under specific circumstances.

- If the period of confidence does not need to be extended after a 15 years;
- If the information has been made public in the time since the information has been accepted in confidence;
- Or with written consent.

Subsection 3 allows, by means of a ministerial order under section 126(2), for the disapplication of this exception to those types or classes of information (which would otherwise be subject to this exception) specified in the ministerial order.

> **68(3)** Subsection (1) does not apply to information of a type or class of information specified in a ministerial order made under subsection 126(2).

SECTION 69 Third party confidential business information

This provision establishes the exception to access to specific types of third party business information that has been "accepted in confidence" by a public body. The *ATIPP Act Regulations* will specify the manner in which information must be accepted by a public body for it to be considered confidential information under this provision.

This section cannot be used in tandem with section 77 Disclosure harmful to third party business interests.

ACCEPTED IN CONFIDENCE only applies when the public body follows the prescribed manner in which to accept information as set out in the *ATIPP Act Regulations*.

This provision only applies to ATIPP requests. If a Public Body accepts information in confidence, it is not released if found responsive to an ATIPP request. It is the public body's responsibility to ensure that confidential information is properly maintained outside of the ATIPP process or risk its release in another manner.

Information that does not meet the threshold for being accepted in confidence can rely on other provisions under this Act that relate to harm, including **section 77(1)** Disclosure harmful to third party business interests.

Subsection 1 states that the head of a public body must refuse to disclose information that would reveal a trade secret; or commercial, financial, scientific or technical information of a third party.

A **"THIRD PARTY"** in respect of an access request, means a person other than the applicant or the responsive public body. A service provider of to a public body is a third party to an access request for the contractor's **proprietary information** and excludes the output/deliverable of the service.

> **69(1)** Subject to subsections (2) and (3), the head of a responsive public body must not grant an applicant access to information held by the responsive public body that
>
> **69(1)(a)** is a trade secret of, or is the commercial, financial, scientific or technical information of, a third party that a public body has, in the prescribed manner, accepted in confidence from the third party; or

Subsection (b) provides for the exception to access to a third party's tax related information. This exception provides that a public body must refuse to disclose information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax. The public body cannot disclose the information unless required to do so by law or by **section 82** (disclosure in the public interest). An example of a required disclosure would be the provision of a tax certificate by municipalities under the authority of the *Municipal Finance and Community Grants Act*.

INFORMATION COLLECTED ON A TAX RETURN is information on a form used to determine taxes to be paid for territorial or federal purposes, and includes corporate, business and personal tax information of a third party.

COLLECTED FOR THE PURPOSE OF DETERMINING TAX LIABILITY means collected for the purpose of determining whether a person or organization owes past, present or future taxes to a municipality or territorial or federal government.

COLLECTED FOR THE PURPOSE OF COLLECTING A TAX means collected by authorities for the purpose of collecting due or overdue taxes for municipality or the provincial or federal government.

The type of information to which section 69(1)(b) may apply includes tax data derived from tax forms, audits of a business intended to determine whether taxes are owed, and information about directors of a bankrupt corporation gathered to determine who should be liable for taxes that are in arrears.

Section 69(1)(b) may not be used to withhold an applicant's own tax information, since this is not information about a third party. Section 69(1)(b) may be used in relation to information

concerning royalties or obtained in the process of collecting royalties. However, such royalties must have a statutory basis as a tax. Where there is doubt about the nature of a royalty, legal advice should be sought.

> **69(b)** was collected by a public body
>
> **69(b)(i)** from a third party's income tax return, or
>
> **69(b)(ii)** for the purpose of determining a tax liability of, or collecting a tax from, a third party.

Subsection 2 allows the head to grant access to third party confidential business information if the third party consents in writing, the information is publicly available information (personal information) or the third party has made the information available to the public.

"PUBLICLY AVAILABLE INFORMATION" means personal information that is:
(a) contained in a public registry,
(b) contained in a magazine, book, newspaper or other similar type of publication that is generally available to the public in print or electronic format, whether by purchase or otherwise, or
(c) of a type or class of personal information prescribed as publicly available information.

> **69(2)** The head of a responsive public body may grant an applicant access to third party information referred to in section (1) if
>
> **69(2)(a)** the third party consents, in writing, to the disclosure of the information;
>
> **69(2)(b)** the third party has made the information available to the public; or
>
> **69(2)(c)** the information is publicly available information.

A third party may consent to the disclosure of some but not all of the information in which the third party has a business interest.

Subsection 3 allows, by means of a ministerial order under **section 126(3)**, for the disapplication of this exception to those types or classes of information (which would otherwise be subject to this exception) specified in the ministerial order. The public interest override in section 82 also applies to this information and access may be granted after considering the factors listed.

> **69(3)** Paragraph (1)(a) does not apply to information of a type or class of trade secret, or of commercial, financial, scientific or technical information, specified in a ministerial order made under subsection 126(3).

Subsection 4 clarifies that information collected for the purposes of a property assessment under the *Assessment and Taxation Act* is not to be considered confidential business information.

> **69(4)** For greater certainty, the information referred to in paragraph (1)(b) does not include information collected by or for a public body under the *Assessment and Taxation Act* for the purpose of an assessment of a property under that Act.

SECTION 70 Third party personal information

This provision establishes a mandatory exception to access to third party personal information. It requires the head to deny access to "personal information" if it would be an "unreasonable invasion of a third party's privacy.

Section 70 of the *Act* protects the privacy of individuals whose personal information may be contained within records responsive to an *ATIPP* request made by someone else. In the exception, the individual the information is about is referred to as a *third party*.

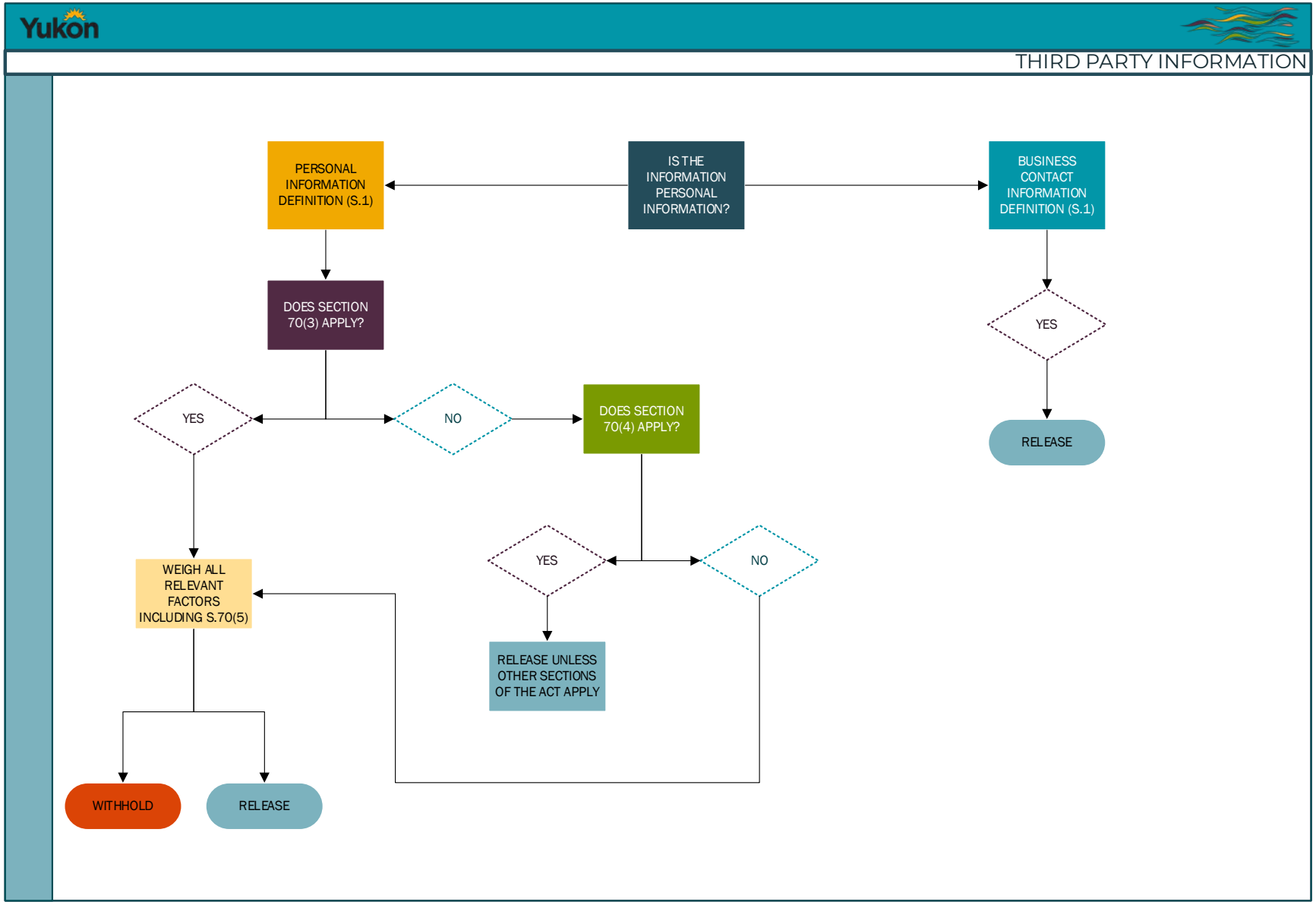
Whenever a request for records includes personal information, as defined in **section 1** of the *Act*, the public body must determine whether disclosure would be an unreasonable invasion of the third party's personal privacy. The examples given are non-exhaustive and do not define personal information in its entirety. Other examples depending on the context might include photographic images, e-mail addresses and an individual's membership in business, professional or benevolent organizations or labour unions.

To qualify as personal information under the *Act*, information must be recorded information about an identifiable individual. The individual may be named in the record or it may be possible to ascertain or deduce the identity of the individual from the contents of the record. Public bodies need to consider the context of a record to determine whether an individual may be identifiable to an applicant who may or may not be aware of a given set of circumstances.

The subsequent provisions set out the factors that the head must consider on a case by case basis when determining whether a disclosure of third party personal information, in response to an access request, would be an unreasonable invasion of a third party's privacy.

If information has been "accepted in confidence" under provisions 68 or 69, information cannot be released unless it meets the subsections outlined in each provision. See **section 68** and **69** for more information.

FIGURE 9.1 THIRD PARTY INFORMATION



Subsection 1 outlines the process the public body uses to determine if releasing if third party personal information will or will not be an unreasonable invasion of personal privacy.

> **70(1)** The head of a responsive public body must not grant an applicant access to a third party's personal information held by the responsive public body if the head determines, in accordance with this section, that disclosure of the information would be an unreasonable invasion of the third party's privacy.
>
> **70(2)** The head must make a determination under subsection (1) in accordance with the following:

Under **subsection (2)(a)** a head must first consider whether the disclosure of the personal information in question is a type of disclosure set out in sub provision 70(3), which are each presumed to be an unreasonably invasion of privacy.

If the head determines that granting access is presumptively an unreasonably invasion of privacy, the head must then weigh the circumstances listed in sub provision 70(5) to conclude whether, in fact, the disclosure is an unreasonable invasion of privacy.

After evaluating the circumstances listed in 70(5), the head may determine that, despite being presumed an unreasonable invasion of privacy under sub provision 70(3), granting access is not an unreasonably invasion of privacy and then the applicant may be granted access to the information.

> **70(2)(a)** a disclosure of a type described in subsection (3) is presumed to be an unreasonable invasion of a third party's privacy that may be rebutted only after the head weighs all relevant factors known to the head in relation to the disclosure, including any factors referred to in subsection (5) that are applicable in the circumstances;

Subsection (2)(b) establishes the rule that those type of disclosures set out in sub provision 70(4) are not an unreasonable invasions of privacy. If one of these cases applies to the information in consideration, the head may not apply this exception to the information (i.e. the head cannot rely on this exception to deny access to the applicant).

> **70(2)(b)** a disclosure of a type described in subsection (4) is not to be considered an unreasonable invasion of a third party's privacy;

Subsection (2)(c) establishes the rules that in respects of the disclosure of information to which neither subsection 70(3) unreasonable invasion of privacy or 70(4) not unreasonable invasion of privacy applies, the head must consider the factors in sub provision 70(5) in determining whether to grant access to the information.

70(2)(c) in the case of any other type of disclosure of a third party's personal information, the head must weigh all relevant factors known to the head in relation to the disclosure, including any factors referred to in subsection (5) that are applicable in the circumstances.

Subsection 3 lists the types of disclosures that are presumed to be an unreasonable invasion of privacy.

70(3) Each of the following types of disclosure of a third party's personal information is considered to be an unreasonable invasion of the third party's privacy:

70(3)(a) the disclosure of information about

70(3)(a)(i) the third party's race, ethnicity, or sexual orientation,

Disclosure of an individual's racial or ethnic origin, or sexual orientation is presumed to be an unreasonable invasion of the third party's personal privacy.

RACIAL ORIGIN means information identifying common descent that connects a group of persons (e.g. Mongolian race or Caucasian descent).

ETHNIC ORIGIN is similar to racial origin in that it identifies a common descent that connects a group of persons but extends to other common attributes such as language, culture or country of origin.

SEXUAL ORIENTATION means information that would identify a person's sexual identity or sexual self-identification.

70(3)(a)(ii) the third party's genetic characteristics or biometric information,

70(3)(a)(iii) the education or employment history of the third party,

Employment history in **subsection (3)(a)(iii)** is a broad, general phrase that covers information pertaining to an individual's work record.

EDUCATIONAL HISTORY refers to any information regarding an individual's schooling and formal training, including names of schools, colleges or universities attended, courses taken, and results achieved.

70(3)(a)(iv) the third party's current or past

70(3)(a)(iv)(A) physical or mental health,

This provision covers records relating to an individual's physical, mental or emotional health, including, for example, diagnostic, and treatment and counselling information. Public bodies that are also custodians under the *Health Information Privacy Management Act* need to comply

with the access request and disclosure provisions of that Act when dealing with health information. For more information, see section 10 in Chapter 2.

70(3)(a)(iv)(B) political or religious beliefs, associations or activities, or

Disclosure of an individual's political, religious beliefs or associations is presumed to be an unreasonable invasion of the third party's personal privacy.

RELIGOUS OR POLITICAL BELIEFS OR ASSOCIATIONS refers to an individual's opinions about religion or a political party, an individual's membership or participation in a church, a religious organization or political party or an individual's association or relationship with a church, a religious organization (including native spirituality), or a political party.

70(3)(a)(iv)(C) amounts or sources of income,

70(3)(a)(v) assets that the third party wholly or partially owns or owned,

70(3)(a)(vi) liabilities for which the third party is or was wholly or partially liable,

70(3)(a)(vii) transactions or banking activities in which the third party is or was involved, or

70(3)(a)(viii) assessments of credit worthiness to which the third party was subject;

Third party financial history, such as assets, liabilities and credit history, falls within the definition of personal information and is also subject to the unreasonable invasion of privacy test.

70(3)(b) the disclosure of information collected from the third party's income tax returns or collected for the purpose of collecting a tax from the third party;

This provision applies to personal information in a form used to calculate or report tax to be paid. PURPOSE OF COLLECTING A TAX means collected by authorities for the purpose of collecting due or overdue federal or territorial taxes.

70(3)(c) the disclosure of information about a discretionary benefit in the nature of income assistance, legal aid or another similar type of benefit that the third party is receiving or has received;

This provision relates to monetary benefits provided by federal or territorial governments to augment an individual's earnings, as well as non-monetary contributions that help supplement earnings from another source. Disclosure of such information is presumed to be an unreasonable invasion of personal privacy.

Subsection (3)(d) applies to individually identifying information in law enforcement records.

> **70(3)(d)** the disclosure of information about a law enforcement matter of which the third party is or was the subject, or about a legal obligation owed to a public body by the third party, if the disclosure occurs during a period in which the information is necessary for use in
>
> **70(3)(d)(i)** an investigation into the matter,
>
> **70(3)(d)(ii)** a prosecution of an offence as it relates to the matter, or
>
> **70(3)(d)(iii)** enforcing the obligation;

"LAW ENFORCEMENT" means policing, which includes criminal or security intelligence operations, a police, security intelligence, criminal or regulatory investigation, including the complaint that initiates the investigation, that leads or could to a penalty or sanction being imposed; or a proceeding that leads, or could lead to a penalty or sanction being imposed.

Disclosure to an applicant of a third party's personal information in a law enforcement record is not presumed to be an unreasonable invasion of privacy if disclosure is necessary to dispose of the law enforcement matter or to continue the investigation. **Subsection (3)(d)** recognizes that a public body that is in possession of evidence relating to a law enforcement matter must have the power to disclose that evidence to the police, another law enforcement agency and to Crown counsel or other persons responsible for prosecuting the offence or imposing a penalty or sanction.

> **70(3)(e)** the disclosure of an individual's opinion or view about the third party that has been provided for the purpose of a recommendation, evaluation or character reference in respect of the third party.

Evaluations and character references are regularly collected by public bodies to assess an individual's employment potential. A formal process of conducting the assessment or evaluation is implied. However, recommendations and character references are also required in situations that do not involve employment. For example, references are generally required by landlords; character references are generally required before placing an individual in a position of trust

Subsection 4 provides types and circumstances of disclosures that are NOT an unreasonable invasion to a third party's personal privacy. In these circumstances, a public body may not rely on section 70 to refuse disclosure of personal information. However, other sections of the *Act* should still be considered when making a decision about disclosure.

> **70(4)** Each of the following types of disclosure of a third party's personal information is not considered to be an unreasonable invasion of the third party's privacy:
>
> **70(4)(a)** a disclosure to which the third party consents in writing;

Consent must be procured in the manner prescribed by the *ATIPP Act Regulations*.

> **70(4)(b)** the disclosure of information of a type of information referred to in paragraph 25(g);

This provision puts a time limit on the protection of privacy after an individual is deceased. This provision is important for permitting historical and genealogical research.

Section 25 Disclosure only if authorized, **subsection (g)** refers to:

- physical or mental health information of an individual who has been deceased for more than 50 years;
- personal information other than physical or mental health information of an individual who has been deceased for more than 25 years, or;
- information contained in a record that has been in existence for 100 years or more or;
- is publically available.

> **70(4)(c)** in the case of a third party who is or was an employee of a public body, the disclosure of information about
>
> **70(4)(c)(i)** the third party's status as an employee of the public body,

Section 1 of the *Act* provides a definition for "business contact information" that is not considered personal information of an individual, and establishes that "employees" include service providers to a public body, that includes volunteers and contractors.

> **70(4)(c)(ii)** the third party's classification or salary range, or the duties and responsibilities of the position or positions that they occupy or occupied as an employee of the public body,

The disclosure of certain employment information about employees of public bodies is not an unreasonable invasion of personal privacy. This provision allows the public body to provide classification levels and job descriptions to the public, through hiring processes and organization charts that are required to be published through Part 3 Division 2 Open Access Information. While salary range and classification is not considered personal information, an employee's exact salary while occupying the position is personal information.

CLASSIFY means to assign (a thing) to a class or category.

"EMPLOYEE" is defined in section 1 of the *Act* as including a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with a public body.

VOLUNTEER means a person who voluntarily takes part in an enterprise or offers to undertake a task and a person who works for an organization voluntarily and without pay.

DUTIES AND RESPONSIBILITIES OF THE POSITION: What an employee has done in his or her professional or official capacity is not personal information, unless the information is evaluative or is otherwise of a "human resources" nature, or there is some other factor which gives it a personal dimension (i.e. makes the information "about" the individual).

Section 70(4)(c)(iv) does not permit the disclosure of information about an employee's performance or conduct, such as an annual performance evaluation or an investigation into an employee's conduct.

Under section 70(4)(c)(ii), it is not an unreasonable invasion of personal privacy to disclose the salary range for an employment position. SALARY means a fixed regular payment made by an employer to an employee. RANGE means a series representing variety or choice; a selection.

An actual salary is not a salary range and therefore cannot be disclosed under section 70(4)(c)(ii), an exact salary may nevertheless be disclosed where it is determined that the disclosure would not be an unreasonable invasion of the third party's privacy.

> **70(4)(c)(iii)** the third party's name as contained in a record prepared by them in the course of their employment with the public body, or
>
> **70(4)(c)(iv)** the third party's opinion or view provided in their performance of the duties and responsibilities of the position or positions that they occupy or occupied other than an opinion or view about another individual;

An employee's opinion that is not about another individual and that is not provided in their performance of the duties and responsibilities of a position is considered personal information under section 1 and it's disclosure may be harmful to personal privacy in certain circumstances.

Licence, permit or other type of authorization of a commercial or professional nature, or a discretionary benefit

Subsection relates to 4(d) the disclosure of information about discretionary benefits granted by a public body to a third party is not an unreasonable invasion of personal privacy. The intent of this provision is to ensure accountability on the part of public bodies with respect to monetary and other benefits that fall within its discretion. Disclosure under this provision is limited to licences, permits or other discretionary benefits relating to a commercial or professional activity, or to real property.

Section 70(4)(d) does not apply to information regarding eligibility for income assistance or social benefits, or regarding the determination of individual benefit levels since these benefits are discretionary; they are calculated according to entitlement formulae.

> **70(4)(d)** in the case of information contained in a record granting, issuing or otherwise providing a licence, permit or other type of authorization of a commercial or professional nature, or a discretionary benefit other than a benefit in the nature of income assistance,

legal aid or another similar type of benefit, that has been granted, issued or otherwise provided to the third party under an Act, the disclosure of the following as specified in that record:

70(4)(d)(i) the name of the third party to whom the licence, permit, authorization or benefit was granted, issued or otherwise provided,

70(4)(d)(ii) the type of licence, permit, authorization or benefit that was granted, issued or otherwise provided,

70(4)(d)(iii) the date on which the licence, permit, authorization or benefit was granted, issued or otherwise provided,

70(4)(d)(iv) if applicable, the period in respect of which the licence, permit, authorization or benefit is or was valid,

70(4)(d)(v) if applicable, the date on which the licence, permit, authorization or benefit expires or expired,

70(4)(d)(vi) in the case of a monetary benefit, the amount of the benefit that was granted or otherwise provided;

This provision enables disclosure of information that reveals details of a discretionary monetary benefit granted to an individual by a public body.

A DISCRETIONARY MONETARY BENEFIT is any monetary allowance that the public body may decide to provide (e.g. a scholarship or a grant).

70(4)(e) in the case of a third party who travelled at the expense of a public body, the disclosure of information about the expenses incurred by the third party, including all payments made to the third party by the public body in relation to the travel;

This provision is linked to public accountability of expenditures that use public funds.

70(4)(f) the disclosure is authorized or required under an Act of the Legislature (including this Act) or of Parliament, or is authorized or required under a regulation made under such an Act;

If an enactment of Yukon or Canada authorizes or requires disclosure, the information must be disclosed where disclosure is provided for in other territorial or federal legislation. For example, the *Environmental Protection and Enhancement Act* lists information that the Department of Environment must, or is authorized to, disclose to the public.

70(4)(g) a disclosure that the head determines is necessary to protect an individual's health or safety.

This provision applies only when there are compelling circumstances affecting the health or safety of any person. To rely on this provision a public body must be able to show that disclosure of the information requested is likely to have a direct bearing on the compelling health or safety matter.

Depending upon the urgency of the compelling circumstances, it may be necessary to consider disclosing third party personal information in the public interest under **section 82** prior to the time that a response to a request is due under Part 3 of the Act.

Subsection 5 sets out the factors that must be weighed by a head, in the applicable cases, in determining whether granting access to the personal information in a specific case is an unreasonable invasion of privacy.

> **70(5)** The following factors are relevant factors to be weighed by the head in relation to a disclosure under subsection (1) (if known to the head and applicable in the circumstances):
>
> **70(5)(a)** the type and sensitivity of the personal information that would be disclosed;
>
> **70(5)(b)** the relationship, if any, between the third party and the applicant;
>
> **70(5)(c)** whether the personal information that would be disclosed is likely to be accurate and reliable;

A public body may have inaccurate personal information in its custody or under its control for a variety of reasons. The personal information may have been incorrectly recorded at the time of collection or compilation or it may have become inaccurate with the passage of time or as a result of a change in circumstances.

For these or other reasons, the public body may be unsure of the reliability of personal information.

> **70(5)(d)** the following factors that are considered to suggest that the disclosure would be an unreasonable invasion of a third party's privacy:
>
> **70(5)(i)** the disclosure would unfairly expose the third party to financial or other harm,

There may be circumstances where disclosure of personal information may mean that the individual involved will be exposed unfairly to monetary loss or injury of a similar nature.

Threat of a civil suit by the applicant against the third party weighs heavily against disclosure. Disruption of family relationships may also constitute harm.

> **70(5)(ii)** the disclosure would unfairly damage the reputation of any person referred to in a record containing the personal information,

UNFAIRLY means without justification, legitimacy or equity.

DAMAGE THE REPUTATION of a person means to harm, injure or adversely affect what is said or believed about the individual's character. An example of information which, if disclosed, would unfairly damage a person's reputation would be allegations of sexual harassment against an individual before an internal investigation is concluded. In some instances, disclosure of the mere fact that a public body maintains a record of a third party may be an unreasonable invasion of a third party's privacy. An example of this could be a probation record. Section 64(3) allows a public body to deny the existence of such records in the response to a request if the denial is reported to the commissioner.

> **70(5)(iii)** the personal information to be disclosed was provided to a public body based on the public body's confirmation that it would hold the information in confidence;
>
> **70(5)(e)** the following factors that are considered to suggest that the disclosure would not be an unreasonable invasion of a third party's privacy:
>
> **70(5)(e)(i)** the disclosure would subject a program or activity, specialized service or data-linking activity of a public body to public scrutiny,
>
> **70(5)(e)(ii)** the disclosure would be likely to promote public health and safety,

The public interests in this provision weigh in favour of disclosure for the purpose of assuring protection of the general public interest.

> **70(5)(e)(iii)** the disclosure is authorized or required under an Act of the Legislature (including this Act) or of Parliament, or is authorized or required under a regulation made under such an Act,
>
> **70(5)(e)(iv)** the disclosure would assist in researching or validating the claims, disputes or grievances of Aboriginal peoples,
>
> **70(5)(e)(v)** the personal information that would be disclosed is relevant to a determination of the applicant's rights.

There may be occasions where the applicant requires access to personal information about someone else in order to assist in determining his or her own rights. Motives for requesting information are not normally relevant to the processing of a request. However, if it appears that the personal information is being requested in order to assist in determining the applicant's rights, it will be necessary for the applicant to confirm that this is the case. The interests of the applicant and the privacy interests of the third party will then have to be weighed to decide whether disclosure of personal information is essential to a fair determination of the applicant's rights.

APPLICANT'S RIGHTS refers to any claim, entitlement, privilege or immunity of the applicant who is requesting someone else's information. For example, disclosure of third party personal

information may be necessary so that an individual can initiate legal proceedings to prove his or her inheritance rights.

SECTION 71 Personnel assessment conducted by or for public body

This provision establishes the exception to access to information about personnel assessments conducted for the head of a public body about employees. A personnel assessment in this section is limited to instances of disrespectful conduct that may result in discipline or termination of employment. It requires a head to refuse to grant access to information about a "personnel assessment" unless the affected employee requests the information and it is contained in a final report S71(3) or its disclosure will not reasonably expected to meet circumstances listed in S71(4).). These exceptions are based on the Public Service Commission's Respectful Workplace Policy (GAM 3.47). **For the purpose of <u>this section</u> employees do not include service providers**.

> **71(1)** In this section, "employee", of a public body, does not include a service provider of the public body; "personnel assessment means a process conducted by or on behalf of an employee's conduct within the public body's workplace or during the performance of their employment duties and responsibilities.
>
> **71(1)(a)** for the purpose of assessing whether the conduct is or has been disrespectful to other employees or the public, and
>
> **71(1)(b)** that may, on the conclusion of the process, result in the discipline or termination, or recommendation for discipline or termination, of the employee.

Subsection 2 establishes the rule that a head must not grant access to a personnel assessment except as provided under sub provision (2) and (3). It clarifies that a third party cannot access a personnel assessment conducted on another individual.

> **71(2)** Subject to subsections (3) and (4), the head of a responsive public body must not grant an applicant access to information held by the responsive public body that is about a personnel assessment.

Subsection 3 requires the head to provide to an affected employee with access to information contained in the final report summarizing the assessment made by the public body.

> **71(3)** The head of the responsive public body must grant an applicant whose conduct has been the subject of a personnel assessment access to information contained in the final report summarizing the personnel assessment other than the following information:
>
> **71(3)(a)** information to which access is prohibited under this Division;

> **71(3)(b)** information to which the head decides to deny the applicant access under Division 9.

Subsection 4 empowers the head to grant the affected employee access to additional information related to the personnel assessment if the disclosure of the information would not result in any of the harms set out in the paragraphs.

> **71(4)** The head of the responsive public body may grant an applicant whose conduct has been the subject of a personnel assessment access to any information created or gathered for the purpose of the personnel assessment if the head is satisfied that the disclosure of the information would not be reasonably expected to
>
> **71(4)(a)** deter employees or the public from bringing forward concerns in respect of what they perceive to be disrespectful conduct within the public service;
>
> **71(4)(b)** harm relationships between employees in the workplace;
>
> **71(4)(c)** reveal information provided to a public body by an individual in accordance with paragraph 80(1)(b);

This provision speaks to information provided by a public body that was accepted in confidence in accordance with *ATIPP Act Regulations* in connection with provision for confidential information provided by individual.

> **71(4)(d)** unfairly damage the reputation of a person referred to in the information; or
>
> **71(4)(e)** prejudice the rights of a person who is involved, or may be reasonably expected to be involved, in a proceeding to which the personnel assessment relates.

In order for **section 71(3)** or **71(4)** to apply, the recommendations, evaluations or references must be about an identifiable individual and must be provided by someone other than that individual.

DIVISION 9 – INFORMATION TO WHICH ACCESS MAY BE DENIED

SECTION 72 Information related to law enforcement

This provision establishes the exception to access to information is related to specific law enforcement and proceedings identified. It allows a head to deny access to this information.

"LAW ENFORCEMENT" means:

- policing, including criminal or security intelligence operations,
- a police, security intelligence, criminal or regulatory investigation, including the complaint that initiates the investigation, that leads or could lead to a penalty or sanction being imposed, or
- a proceeding that leads or could lead to a penalty or sanction being imposed

"PROCEEDING" means (a) in respect of a court, a civil or criminal proceeding, or (b) in respect of an adjudicator, the hearing of a matter over which the adjudicator is authorized under an Act of the Legislature or of Parliament to preside.

POLICING refers to the activities of police services. This means activities carried out under the authority of a statute regarding the maintenance of public order, detection and prevention of crime or the enforcement of law.

CRIMINAL INTELLIGENCE is information relating to a person or group of persons. It is compiled by police services to anticipate, prevent or monitor possible criminal activity. Intelligence-gathering is sometimes a separate activity from the conduct of investigations. Intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, or to ensure the security of individuals or organizations.

INVESTIGATION has been defined, in general, as a systematic process of examination, inquiry and observation.

A public body need not carry out the investigation for that investigation to meet the definition. The investigation might be carried out by a police service on behalf of the public body. If the requested records are not within the custody or control of the public body to which the request is made, that public body is not required to search for responsive records in the custody or under the control of another public body.

Section 72 is a discretionary exemption. See Overview at beginning of this chapter.

72(1) Subject to subsection (2), the head of a responsive public body may deny an applicant access to information held by the responsive public body if the head determines that disclosure of the information

71(1)(a) could reasonably be expected to reveal

71(1)(a)(i) the existence of a record that was confiscated from a person by a peace officer under an Act of the Legislature or of Parliament,

71(1)(a)(ii) information contained in a correctional record that a public body has, in the prescribed manner, accepted in confidence, or

71(1)(a)(iii) the identity of a confidential source, or information that the source is providing or has provided, to a public body in respect of a law enforcement matter; or

72(1)(b) could reasonably be expected to

72(1)(b)(i) interfere with a law enforcement matter,

72(1)(b)(ii) reduce the effectiveness of an investigative technique or procedure used or likely to be used in law enforcement,

72(1)(b)(iii) adversely affect the position or legal rights of the Government of Yukon or a public body in respect of an existing or anticipated proceeding to which the Government of Yukon or the public body is, or is expected to be, a party,

72(1)(b)(iv) harm the reputation of a person or organization referred to in a report prepared for the purpose of a law enforcement matter,

72(1)(b)(v) compromise the defence of Canada or a foreign state allied to or associated with Canada, or jeopardize the detection, prevention or suppression of espionage, sabotage or terrorism,

72(1)(b)(vi) adversely affect the security of property or a system, including a building, vehicle, computer system or communications system,

72(1)(b) (vii) facilitate the escape from custody of an individual who is lawfully detained,

72(1)(b)(viii) aid in the commission of, or interfere with the control of, an unlawful act or a crime,

72(1)(b)(ix) endanger the life of, or threaten the safety of, a law enforcement officer,

72(1)(b)(x) expose the author of a record relating to a law enforcement matter, or a person who is quoted in the record, to civil liability, or

72(1)(b)(xi) deprive a person of their right to a fair trial or impartial adjudication.

Subsection 2 requires the release of information that may be required to be deposited into the Open Access Register under **Part 3 Division 2**, Open Access Information.

72(2) The head of a responsive public body must not deny an applicant access to information held by the responsive public body that is contained in

72(2)(a) a final report in respect of a routine inspection or other compliance activity carried out by a public body under an Act;

72(2)(b) a record that provides a general outline of the organizational structure of a law enforcement agency, including a description of its programs or activities; or

72(2)(c) a final report about the degree of success or efficiency of a law enforcement program or activity of a public body unless the head decides that there is reason to deny the applicant access to information in accordance with subsection (1).

SECTION 73 Information subject to legal privilege

This provision establishes the exception to access to information that is subject to a legal privilege. It also provides for an exception to access to information that has been prepared for the Attorney General or a public body in respect of matters related to legal service or prosecutions that may not be subject to legal privilege, or communications between the Attorney General and a public body in respect of these matters with any other person and the Attorney General or a public body.

"ATTORNEY GENERAL" means the minister who is the Attorney General of Yukon under section 3 of the Department of Justice Act and includes a lawyer, agent or delegate acting for or on behalf of the Attorney General.

"LEGAL PRIVILEGE" means solicitor-client privilege, litigation privilege or any other type of legal privilege (including a privilege of the law of evidence).

The intent of section 73 is to ensure that information privileged at law, as well as other similar information in the custody or under the control of a public body, is protected from disclosure in much the same way as an individual's information would be by his or her own lawyer.

The following is a non-exclusive list of indicators that, if present, suggest that section 73 might apply:

- the record is a letter, fax, e-mail or other correspondence to or from the public body's lawyer, including a lawyer at the Department of Justice and Attorney General (for government departments and agencies);
- the record is attached to correspondence to or from a lawyer;
- the record is a note documenting legal advice given by a lawyer or a statement of account from a lawyer that details the services provided by the lawyer;
- the information was provided by a confidential informant;
- the information relates to an existing or contemplated lawsuit;
- the information relates to a criminal prosecution;
- the record relates to a public body's investigation of a third party; or
- the record relates to the operations of the Legislative Assembly.

If one or more of these indicators exist, section 73 may apply. Public bodies should consider consulting with legal counsel when a record contains information that may qualify for exception under section 73 and the public body is unsure whether to claim its legal privilege. The first step is to determine whether legal privilege applies. The next step is to decide whether the privilege should be waived.

Section 73 is a discretionary exception. See overview at beginning of this chapter.

> **73** The head of a responsive public body may deny an applicant access to information held by the responsive public body that
>
> **73(a)** is subject to a legal privilege of a public body or any other person;

Subsection (a) gives a public body the discretion to refuse to disclose information that is subject to any type of legal privilege. There are several types of legal privilege that include:

- solicitor–client privilege;
- litigation privilege;
- common interest privilege;
- parliamentary privilege;
- police informer privilege;
- case-by-case privilege for private records and for Crown records;
- settlement negotiation privilege; and
- statutory privilege.

If one of these privileges applies, the information may be withheld under this subsection. Public bodies should note that, since **subsection (a)** is a **discretionary exception**, the Information and Privacy Commissioner will not raise it as an exception to disclosure if the public body does not.

> **73(b)** has been prepared by or for the Attorney General or a public body in respect of
>
> **73(b)(i)** the provision of legal service to or by the Attorney General, or
>
> **73(b)(ii)** the prosecution of an offence by the Attorney General; or
>
> **73(c)** is contained in a communication about the provision of legal services or a prosecution referred to in paragraph (b) between
>
> **73(c)(i)** the Attorney General or a public body, and
>
> **73(c)(ii)** any other person.

SECTION 74 Policy Advice and Recommendations

This provision deals with exceptions for requests to access to information if the head determines that the disclosure of that information would reveal things such as advice or recommendations developed by or for a public body or a minister; information contained in an auditor's draft audit that has been in existence for less than two years; and types of information that is policy advice and recommendations to which this exception does not apply.

ADVICE includes the analysis of a situation or issue that may require action and the presentation of options for future action, but not the presentation of facts.

RECOMMENDATIONS includes suggestions for a course of action as well as the rationale for a suggested course of action.

Section 74 is a discretionary exemption. See Overview at beginning of this chapter.

> **74(1)** Subject to subsection (2), the head of a responsive public body may deny an applicant access to information held by the responsive public body if the head determines that disclosure of the information would reveal
>
> **74(1)(a)** advice or recommendations prepared by or for a public body or a minister; or

This provision is intended to allow for thorough discussion of policy issues that otherwise may not occur if the deliberative process were subject to excessive scrutiny.

Note: Cabinet records are information to which access is prohibited. See **section 67** of the Act for more information.

Subsection (1)(b) allows the head to deny access to information contained in an auditor's draft audit that has been in existence for less than two years.

The time requirement relates to final audits that must be granted access (see subsection (2)(b)) and any draft audit report that is older than two years.

> **74(1)(b)** information contained in an auditor's draft audit report that has been in existence for less than two years.

"AUDITOR" means (a) the individual appointed by Parliament as the Auditor General of Canada, (b) the individual appointed under the *Financial Administration Act* as the internal auditor, or (c) any other person prescribed as an auditor.

Subsection 2 sets out the types of information that is policy advice and recommendations to which this exception does not apply. This subsection links to the requirements for ministerial public bodies to publish information in the Open Access Register under the Open Access part of the Act.

"OPEN ACCESS REGISTER", of a public body, means the open access register established under paragraph 41(1)(a).

> **74(2)** The head of a responsive public body must not deny an applicant access to information and records of the following types held by the responsive public body:
>
> **74(2)(a)** factual information included in a record to which subsection (1) applies only for the purpose of providing contextual background information;
>
> **74(2)(b)** an auditor's final audit report;
>
> **74(2)(c)** information contained in an auditor's draft audit report that has been inexistence for two years or more;
>
> **74(2)(d)** a final report, of a type other than an auditor's final audit report, on the

performance or efficiency of a public body or any of its programs or activities, or specialized services;

74(2)(e) a final report by a statutory body or any other body established (whether or not under an Act) for the purpose of providing advice or recommendations to the public body in respect of any of its policies, programs or activities, specialized services or data-linking activities;

74(2)(f) an appraisal report in relation to the value or condition of public property;

74(2)(g) a feasibility or technical study (including related cost estimates) about a policy or project of a public body;

74(2)(h) a report on the results of field research conducted by or for a public body whether or not a policy proposal to which the report relates has been formulated or determined;

74(2)(i) a plan or proposal to establish a new program or change an existing program if the plan or proposal has been approved or rejected by the head of a public body;

74(2)(j) an environmental report about an environmental test conducted by or for a public body;

74(2)(k) a consumer test report or product test report conducted by or for a public body;

74(2)(l) a final report on the economic or financial status of the Government of Yukon or a public body;

74(2)(m) a statement of the reasons for a decision made by a public body that affects a legal right of the applicant;

74(2)(n) information that the head of a public body has cited publicly as the basis for making a decision or formulating a policy of the public body;

74(2)(o) information referred to in subsection (1) that has been in existence for 10 years or more.

SECTION 75 Disclosure harmful to economic or financial interests of public body

This provision allow the head to deny access to information which could harm the financial or economic interests of a public body.

Subsection (1) of the *Act* provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body or Government of Yukon as a whole, or the ability of the Government to manage the economy.

This recognizes that public bodies, individually or collectively, may hold significant amounts of financial and economic information that is critical to the management of the Yukon economy. Subsection (1) ensures that, where harm would result from disclosure of information, the information may be withheld.

Section 75 is a discretionary exemption. See Overview at beginning of this chapter.

Harms test

In order to use the exception, a public body must have objective grounds for believing that disclosure will likely result in harm.

3 part harms test:

1) There must be a reasonable expectation of probable harm;
2) The harm must constitute damage or detriments, and not mere inconvenience; and
3) There must be a causal connection between disclosure and the anticipated harm.

The evidence must demonstrate a probability of harm from disclosure and not just a well-intentioned but unjustifiably cautions approach to the avoidance of any risk whatsoever because of the sensitivity of the matters at issue. The likelihood of harm must be genuine and conceivable.

The harm must pass a general threshold of damage or detriment, not mere interference and hindrance. The threshold may vary depending on the nature of the harm that may result from disclosure. The harm must be specific to the context of the request.

For more information on harms tests and applying exceptions, see the Overview at the beginning of this chapter.

The context in which a public body operates should be taken into account in determining whether it is reasonable to expect that harm will result from the disclosure of the information. In applying this exception, public bodies should take into account not just the specific harm that could occur as a result of disclosure of the information (i.e. **section 75(1)(a) to (b))** but also whether the broader economic interests of the public body or the Yukon Government would be harmed.

Section 75(2) provides that a public body must not refuse to disclose under **section 75(1)** the results of product or environmental testing carried out by or for a public body, unless the testing was done:

- for a fee as a service to a person, other than the public body **(section 75(2)(a));** or
- for the purpose of developing methods of testing or testing products for possible purchase **(section 75(2)(b)).**

ECONOMIC INTERESTS refers to both the broad interests of a public body and, for provincial public bodies, of the government as a whole, in managing the production, distribution and consumption of goods and services. The term also covers financial matters such as the management of assets and liabilities by a public body and the public body's ability to protect its own or the government's interests in financial transactions.

The FINANCIAL INTERESTS of the Government of Yukon include the ability to collect taxes and generate revenues.

Harm to these interests includes damage or detriment to the economic policies or activities for which a single public body is responsible, as well as harm to policies and programs that affect the overall economy of. Harm to these interests also includes monetary loss or loss of assets with monetary value.

Examples of information to which the exception in **section 75** may apply include:

- information on a public body's investment strategies which could affect its interests or future financial position;

- information in budget preparation documents which could result in segments of the private sector taking actions affecting the ability of the government or a local public body to meet economic goals;

- information about licensing and inspection practices of a public body which could affect the amount of revenue collected; and

- information about a trade deal, a development plan or strategy or an economic negotiation that has not been completed.

The phrase ABILITY TO MANAGE THE ECONOMY refers to the responsibility of the Government of Yukon to manage the territory's economic activities by ensuring that an appropriate economic infrastructure is in place, and by facilitating and regulating the activities of the marketplace. This depends on a range of activities, including fiscal and economic policies, taxation, and economic and business development initiatives.

> **75(1)** Subject to subsection (2), the head of a responsive public body may deny an applicant access to information held by the responsive public body that could reasonably be expected to harm the financial or economic interests of the Government of Yukon or of a public body, or the ability of the Government of Yukon to manage the economy, including the following information:
>
> **75(1)(a)** information that is

Subsection (a)(i) allows the head to deny access to information that is a trade secret of a public body or the Government of Yukon

> **75(1)(a)(i)** a trade secret of the Government of Yukon or a public body,

Subsection (1)(a)(i) does not apply to trade secrets of a third party. Requirements relating to the protection of these trade secrets are dealt with in **section 77(1)**. If this type of information from a third party was accepted in confidence in the manner prescribed under **section 69** it may only be released if it meets the criteria outlined in **sections 69(2)-(3)**.

Subsection (1)(a)(ii) allows the head to deny access to information that is commercial, financial, scientific or technical information of a public body.

> **75(1)(a)(ii)** commercial, financial, scientific or technical information of the Government of Yukon or a public body and that has, or is reasonably likely to have, monetary value,

The exception in this provision is subject to a three-part test. In order for the exception to apply, all of the following conditions must be met:

- the information must be financial, commercial, scientific, technical or other information;
- the public body or the Government of Yukon must have a proprietary interest or a right of use; and
- the information must have, or be reasonably likely to have, monetary value.

The second part of the test for this exception requires that the public body or the Government of Yukon to have a proprietary interest in the information. This means that the public body or the government must be able to demonstrate rights to the information. For example, a public body may have a proprietary interest in geographical information systems mapping data or statistical data.

The third part of the test is whether the information has or is reasonably likely to have monetary value. Monetary value may be demonstrated by evidence of potential for financial return to the public body or government. An example of information that is reasonably likely to have monetary value might include a course developed by a teacher employed by a school board.

Subsection (1)(iii) allows a head to deny access to information related to the management of personnel that has not been implemented. ‘Management of personnel’ includes all aspects of managing human resources, for example, plans around a reorganization, including changes to job classifications.

> **75(1)(a)(iii)** a plan relating to the management or administration of the personnel of a public body that has not been fully implemented by the public body, or
>
> **75(1)(a)(iv)** a position, plan, procedure or instruction, or estimates or criteria, developed for the purpose of contractual or other negotiations (including land claims and self-

government negotiations, and labour relations negotiations) by or on behalf of the Government of Yukon or a public body; or

75(1)(b) information the disclosure of which the head determines could reasonably be expected to

Subsection (1)(b)(i) allows the head to deny access to information that could prejudice the financial or economic interests of a public body.

75(1)(b)(i) prejudice the financial or economic interests of the Government of Yukon or a public body, or

Subsection (1)(b)(ii) allows the head to deny access to information that would result in significant financial loss or gain to a third party due to the premature disclosure of information.

This is intended to cover information about a proposal or project that has not been made public and would result in a monetary loss or gain to an organization other than the public body.

75(1)(b)(ii) result in a significant financial loss or gain to a third party caused by premature disclosure of a pending decision of the Government of Yukon or a public body.

In the case of FINANCIAL LOSS, there must be reasonable grounds to believe that disclosure of information in the specific record would result in direct monetary or equivalent loss.

Subsection 2 requires the head to disclose information related to environmental testing.

75(2) The head of a responsive public body must not deny an applicant access to information about the results of product or environmental testing carried out by or for a public body unless the testing was done

75(2)(a) as a service for a person other than a public body; or

75(2)(b) for the purpose of developing methods of testing.

The intent of the provision is to ensure that a public body does not withhold information resulting from product or environmental testing carried out either by the employees of a public body or on its behalf by another organization. Examples include information on products such as air filters, environmental test results on water quality or air quality and commercial product testing and soil testing.

Information can be withheld when the public body performs the testing, for a fee, as a service to a private citizen or private corporate body.

The information may also be withheld if the testing was done for the purpose of developing testing methods, such as a new methodology for tire recycling.

The exception can also be used to withhold test results compiled to determine whether or not a public body would purchase a product.

SECTION 76 Disclosure harmful to intergovernmental relations

Subsection (1) allows the head to deny access to information that could harm relations between Government of Yukon (including a public body) and the other government or organization (see **section 68(1)** for the list of organization this exception applies to). These provisions are intended to protect the release of information that could cause damage to the conduct of relations. For example, the premature release of a memo from the Government of Canada that summarizes the terms of an agreement that has not been made public.

This provision is discretionary. See overview at beginning of chapter.

> **76(1)** Subject to subsection (2), the head of a responsive public body may deny an applicant access to information held by the responsive public body that a public body has not accepted in confidence in the prescribed manner from a government or organization referred to in subsection 68(1) if the head determines that disclosure of the information could reasonably be expected to harm relations between the Government of Yukon or a public body and the other government or organization.

If information has not been "accepted in confidence" under **section 68**, the public body must use the necessary harms test discussed in the Overview at the beginning of this chapter.

Harm to intergovernmental relations: This provision applies to information that if disclosed could reasonably be expected to harm relations between the Government of Yukon and the listed external government entities:

- Government of Canada
- A province (definition includes territory)
- A foreign state
- A First Nation government
- A municipality
- An international organization of states

The exception may apply to information that relates to current or future relations.

RELATIONS is intended to cover both formal negotiations and more general exchanges and associations between the Government of Yukon and other governments or their agencies.

HARM means damage or detriment to negotiations and general associations and exchanges. To satisfy the harms test, there must be a reasonable probability that disclosure would harm

and not merely hinder, impede or minimally interfere with the conduct of intergovernmental relations or negotiations.

"FIRST NATION GOVERNMENT" is defined in section 1 as:

- A governing body established under the constitution of a Yukon First Nation,
- The council of a band recognized under the Indian Act (Canada), or
- An entity prescribed as a First Nation government.

A foreign state refers to the government of any foreign nation or state, including the component state governments of federated states.

An international organization of states refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples include the United Nations and the International Monetary Fund.

Subsection 2 requires information that is older than 15 years or more, but excludes information related to land claims.

> **76(2)** The head of a responsive public body must not deny an applicant access to information referred to in subsection (1) that has been in existence for 15 years or more unless the information is about or related to land claims or self-government negotiations that have not concluded between the Government of Yukon and another government or organization.

To determine whether a time limitation applies to a record or information, the public body would compare the number of years stated (15), with the date and month on the record. To apply this subsection, at least 15 years must have elapsed since the record was created.

Where the date of the creation of the record is not obvious, the public body would have to examine the context of the record, other documents that may be in proximity to the record in a file or which may refer to the record and other facts that may help provide a date. Information in a record that fits within an exception under the Act, but that is older than the 15 year time limitation must be disclosed unless another exception provision applies.

SECTION 77 Disclosure harmful to third party business interests

This discretionary provision allows the head to deny an applicant access to information that would harm a third party's business interests. This provision is intended to capture information that a public body may hold that was **not** "accepted in confidence" in accordance with section 69.

The application of this provision is restricted to information that is a trade secret, commercial, financial, scientific or technical information of a third party.

The head must determine that at least one of the harms listed will be triggered in order for the information to be refused. More than one harm may be applicable and could be cited.

> **77(1)** Subject to subsections (2) and (3), the head of a responsive public body may deny an applicant access to information held by the responsive public body that is a trade secret of, or commercial, financial, scientific or technical information of, a third party that a public body has not accepted in confidence in the prescribed manner from the third party if

> **77(1)(a)** the head determines that disclosure of the information could reasonably be expected to result in undue financial loss or gain to a person or entity;

This harm would result in any undue financial loss or gain to an organization or entity. The loss or gain would be a monetary loss or gain.

> **77(1)(b)** the head determines that disclosure of the information could reasonably be expected to result in similar information no longer being supplied to the responsive public body and the head is satisfied that it is in the public interest that similar information continue to be supplied to the responsive public body;

This harm would result in the third party no longer supplying information to the public body that is similar to the information being disclosed - information that was voluntarily supplied by a business is no longer supplied.

> **77(1)(c)** the head determines that disclosure of the information could reasonably be expected to significantly harm the competitive or negotiating position of the third party; or

This would result in harm towards the competitive or negotiating position of the third party. Harming the competitive position could include information a competitor could find valuable; for example, marketing plans or information that reveal the internal workings of a company. Harming the negotiating position could include a document which discloses the lowest price a company will offer in the acquisition of assets, during the negotiation for the purchase of those assets.

> **77(1)(d)** the head determines that disclosure of the information could reasonably be expected to harm or interfere with the work of an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

This harm could interfere with the work of a person appointed to resolve or inquire into a labour relations matter.

Subsection 2 sets out the factors the head must consider before deciding to deny access. These include the results of any third party consultations undertaken under section 59(1)(a) and whether the access to the information would promote public health and safety.

> **77(2)** Before denying access to information under subsection (1), the head of a responsive public body must consider
>
> **77(2)(a)** the objections of a third party, if any, submitted in accordance with a notice provided to the third party under paragraph 59(1)(a); and
>
> **77(2)(b)** whether, despite any objections, granting the applicant access to the information would promote public health or safety.

Subsection 3 requires the head to allow access to information if the third party consents in writing, if an Act requires the disclosure, or the information has been made publicly available.

> **77(3)** The head of a responsive public body must grant an applicant access to information referred to in subsection (1) if
>
> **77(3)(a)** the third party consents, in writing, to the disclosure;
>
> **77(3)(b)** the third party has made the information available to the public;
>
> **77(3)(c)** an Act of the Legislature or of Parliament authorizes or requires the disclosure of the information; or
>
> **77(3)(d)** the information is publicly available information.

SECTION 78 Disclosure harmful to conservation or heritage site

Section 78 provides that a public body may refuse to disclose information that could reasonably be expected to damage or interfere with the conservation or preservation of

- A fossil or site related to anthropological, cultural or heritage value
- A threatened or vulnerable species of plant or animal
- Any rare, threatened, endangered or vulnerable living resource.

For this discretionary exemption to apply, there must be objective grounds to believe that a disclosure is likely to result in damage or interference with conservation or preservation measures.

Damage refers to destruction, disturbance, alteration, deterioration or reduction in the value of an historic resource.

Section 78 is a discretionary exemption. See Overview at beginning of chapter.

> **78** The head of a responsive public body may deny an applicant access to information if the head determines that disclosure of the information to the applicant could reasonably be expected to result in damage to, or interference with, the conservation or preservation of
>
> **78(a)** a fossil, or a natural site that has, or is likely to have, anthropological, cultural or heritage value;

Historic resources

Subsection (a) enables a public body to withhold information about historic resources when it is assessed that a disclosure could result in damage to these resources, or interference with conservation measures. If a public body has records which may fall under this exception, it may consult with the department responsible for the *Historic Resources Act* (Tourism and Culture) in making a decision on the disclosure.

The *Historic Resources Act* defines historic resource as a historic site, object or any work or assembly of works in nature or of human endeavour that is of value for its archaeological, palaeontological, pre-historic, historic, scientific or aesthetic features.

> **78(b)** a species of plant or animal that is endangered, threatened or vulnerable; or
>
> **78(c)** any other rare, threatened, endangered or vulnerable living resource.

Endangered, threatened or vulnerable species

Under **subsection (b)**, the following general definitions apply.

A *rare species* is a species of flora or fauna that is in a special category because it does not occur in great abundance in nature, either because it is not prolific or its population or range has been adversely affected by time, modern civilization, climate change or predators.

An *endangered species* is any species of flora or fauna that is threatened with extinction throughout all or a significant portion of its natural range.

A *threatened species* is any species of flora or fauna that is likely to become endangered in Canada or Yukon if the factors affecting its vulnerability are not reversed.

A *vulnerable species* is any species of flora or fauna that is of concern because it is naturally scarce or likely to become threatened as a result of disclosure of specific information about it.

SECTION 79 Disclosure harmful to individual or public

This provision allows the public body to deny the applicant access to information that could reasonably cause them harm, either to their physical or psychological heath.

The exception may extend to an applicant's own personal information as well as to information about third parties.

In order to determine whether a threat to the safety, mental or physical health of any person exists, a public body must apply the harms test. There must be evidence of a reasonable expectation of probable harm; the harm must constitute damage or detriment; and there must be a causal connection between disclosure and the anticipated harm.

For more information on the harms test see the Overview at the beginning of this chapter.

THREATEN means to expose to risk or harm, and safety implies relative freedom from danger or risks.

INTERFERENCE WITH PUBLIC SAFETY would occur where the disclosure of information could reasonably be expected to hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public at large.

> **79** The head of a responsive public body may deny an applicant access to information held by the responsive public body (including the applicant's own personal information)
>
> **79(a)** if the head reasonably believes that disclosure of the information to the applicant could reasonably be expected to
>
> **79(a)(i)** cause serious harm to the health of, or threaten the safety of, an individual, or

This provision allows the head to deny access to information that could harm an individual's health or safety, for example, refusing to disclose the location of a transition house or the identity of a whistleblower who has expressed opinions of wrongdoing.

> **79(a)(ii)** threaten public health or safety; or

This provision allows the head to deny access to information which may threaten public health or safety, for example, the release of environmental tests taken with faulty equipment. The false results would lead to widespread panic.

> **79(b)** in the case of disclosure to the applicant of the applicant's own personal information, if a medical practitioner, nurse practitioner, registered nurse or other qualified health care professional has provided their opinion to the head that the

> disclosure could reasonably be expected to cause serious harm to the health of, or threaten the safety of, the applicant.

This provision allows the head to deny personal information to the applicant if a certified medical professional believes the disclosure could cause harm to the applicant's health or safety. This means serious physical injury, mental trauma or danger to the applicant that could reasonably be expected to ensue directly from disclosure of the personal information. The decision must be supported by the opinion of a medical practitioner, nurse practitioner, registered nurse, or any other qualified health care professional, depending on the circumstances of the case.

An example where this exception may be relevant is where an individual with a long and difficult history of mental instability might suffer grave mental or physical trauma if certain diagnoses were made available to him or her without the benefit of medical or mental health intervention.

SECTION 80 Confidential information provided by individual

Section 80 is a discretionary exception and applies only when an individual is requesting their own, or another individual's personal information. The exception applies to both the applicant's own personal information and the personal information of the individual supplying the evaluation or opinion. The exception is intended to preserve the candour of the evaluative information or opinions.

Subsection 1 allows the head to deny access to an applicant's own personal information. This is intended to preserve the forthrightness of the required evaluative material needed to make a determination in the instances below.

> **80(1)** Subject to subsection (2), the head of a responsive public body may deny an applicant access to information that
>
> **80(1)(a)** an individual provided to the responsive public body for the purpose of determining the individual's or another individual's suitability, eligibility or qualifications for
>
> **80(1)(a)(i)** potential employment with the responsive public body, or

This provision allows the head to deny access to the disclosure of information provided by an individual for potential employment by a public body, such as information compiled about an individual's strengths or weaknesses or qualifications.

Examples of information to which **section 80(1)(a)(i)** may apply include:

- a verbatim transcription of a reference check of an employment candidate;
- a summary of a mix of telephone and written reference checks compiled by a public body employee;
- recorded comments from a third party who is not a referee for a candidate but makes the comments in the same employment context in which a reference letter would be provided, and
- handwritten notes taken by an interviewer during the recruitment process.

Personnel assessments conducted by or for a public body to assess whether an employee's conduct in the workplace has been disrespectful to other employees or the public are covered under the provision, **Section 71.**

> **80(1)(a)(ii)** an honour or award, including a scholarship, bursary or honorary degree; or

This provision allows the head to deny access to the disclosure of information provided by an individual that is used to determine whether an individual can receive an honour or award.

Subsection (b) allows the head to refuse to disclose personal information, including any information that would identify an individual, if the information was "accepted in confidence", in accordance with regulation. Please see *ATIPP Act Regulations* for more information.

For example, individuals are providing information about disrespectful conduct who do not wish to be identified or an individual is supplying traditional knowledge to the public body and they do not wish this information to be disclosed for another purpose.

> **80(b)** an individual provided to a public body after the public body's confirmation, in the prescribed manner, that it would hold in confidence the information or the identity of the individual.

Subsection 2 allows means of a ministerial order under **section 126(4)**, for the disapplication of this exception to those types or classes of information (which would otherwise be subject to this exception) specified in the ministerial order.

> **80(2)** Subsection (1) does not apply to information of a type or class of information specified in a ministerial order made under subsection 126(4).

For more on ministerial orders specifying reputable public sources, see **section 126**.

SECTION 81 Information to become publicly available

This provision allows the head to deny access to information if it will be made publicly available within 90 days from the time an ATIPP request was made.

Section 81 is a discretionary exception. See Overview at beginning of chapter.

> **81** The head of a responsive public body may deny an applicant access to information if the information
>
> **81(a)** is to become publicly available information within 90 days after the activation date for the applicant's access request, or
>
> **81(b)** is to be otherwise made available to the public, within 90 days after the activation date for the applicant's access request.

This provision allows a public body to decide whether or not to withhold information that will be published or released within 90 days of the activation date of the applicant's request.

Situations arise when a request is made for information that is about to be published. There may be a number of reasons to withhold the information under **section 81(b).** For example, where a publication is required to be tabled in the Legislature, it may be appropriate for the Minister or head to exercise his or her discretion not to release the information first through the *ATIPP Act*. It may also be reasonable to not disclose the information through the *ATIPP Act* if the information is scheduled to be released in conjunction with a public event or public announcement or is to be published within 90 days of the applicant's request.

The 90 days for publication or release is from the date of receipt of the activation date of the applicant's access request and not from the date when a response is made to the request. It is important that a public body ensure that the requested records will be published or released to the public within the 90-day time frame established by the provision

If an applicant requests information to which this exception applies, the public body should inform the applicant how the information may be accessed

DIVISION 10 – PUBLIC INTEREST OVERRIDE AND MANDATORY DISCLOSURE

SECTION 82 No denial of access if access clearly in public interest

This provision authorizes a general public interest override if a disclosure is in the public's interest. These provisions require the head to determine whether to refuse information or records using the factors listed in 2(a) and (b). The public interest override provisions apply to all of the exceptions, excluding provision 67 – cabinet confidence. Cabinet confidence was excluded as the Secretary of the Executive Council has the ability to make cabinet information available under **section 67(3)**.

This general provision is intended to cover the situation where the head of a public body may decide that disclosure of information is in the public interest in response to an access request. If the head decides that disclosure is clearly in the public interest the public body must release the information. **Section 43** also allows the head to proactively publish this information as Open Access Information.

Disclosure of the information must be CLEARLY IN THE PUBLIC INTEREST. This determination must be made on a case-by-case basis. Public bodies must balance the public interest in releasing the information with the public and private interests in protecting the information. The requirement that disclosure of the information must be clearly in the public interest means that the information must relate to a matter of compelling public interest, and not just be of interest or of curiosity to the public, a group of people, or individuals. What constitutes a compelling public interest is defined narrowly.

The following are some examples where disclosure may clearly be in the public interest:

- a public body has been alerted about a contagious disease or about an individual who is the carrier of a contagious or dangerous disease;
- a violent or dangerous offender has been released into the community;
- an individual seeking employment in child care on the basis of a false resumé is found to have a history of child molestation that is recorded in a register of employment references for child-care workers; and
- information has come to light about corruption or serious misuse of public funds.

82(1) Despite any provision of Division 8 or 9 other than section 67, the head of a responsive public body must not deny an applicant access to information in relation to which the head, after consideration of the factors listed in paragraphs (2)(a) and (b),

> determines that the public interest in disclosing the information clearly outweighs the public interest in withholding the information from disclosure.

"APPLICANT", in respect of an access request, means the person who submits the access request.

> **82(2)** In determining whether the public interest in disclosing the information clearly outweighs the public interest in withholding it under subsection (1)
>
> **82(2)(a)** the head must consider the following factors:
>
> **82(2)(a)(i)** the level of public interest in the information,

This factor relates to the level of public interest, for example, if a policy decision has a widespread and significant impact on the public, or if there is public interest in informing the debate on the issue.

> **82(2)(a)(ii)** whether the information is likely to be accurate and reliable,

This factor relates to assessing whether the information is accurate or reliable. If it is not, disclosing the information could result in misleading the public.

> **82(2)(a)(iii)** whether similar information is in the public domain,

The head should consider if the information is similar to information already in the public domain **("PUBLICLY AVAILABLE INFORMATION")**; this would assign less weight to releasing it.

> **82(2)(a)(iv)** whether suspicion is likely to exist in respect of a public body's conduct in relation to the matter to which the information relates,

This factor relates to whether there is a wider public interest in clarifying an issue for the public if the release would restore confidence in the public body. By presenting a full picture of the issue, the public will be aided in understanding the public body's decisions to address concerns about misrepresentations of the information.

> **82(2)(a)(v)** if harm to a person, public body or government is likely to result from disclosure of the information, the significance and type of the harm,

This factor relates to the head considering whether any harm will result to an individual, for example, reputational harm or humiliation.

> **82(2)(a)(vi)** whether the disclosure of the information is likely to result in similar information no longer being supplied to a public body;

The head must consider whether the disclosure is likely to result in similar information no longer being provided to a public body.

The factors in **subsection (2)(b)** relate specifically to confidential business information that was accepted in confidence (s. 69(1)).

The head must consider these factors and decide if the public interest in transparency outweighs withholding the information, as listed in 82(b)(i)(A)(B).

> **82(2)(b)** if the information is of a type referred to in paragraph 69(1)(a) or (b), the head must consider the following factors in addition to the factors referred to in paragraph (a):
>
> **82(2)(b)(i)** whether the public interest in disclosing the information clearly outweighs
>
> **82(2)(b)(i)(A)** any financial loss or gain to a person or entity that could be reasonably expected to occur because of the disclosure, or
>
> **82(2)(b)(i)(B)** any harm to the competitive or negotiating position of a person or entity that could be reasonably expected to occur because of the disclosure,
>
> **82(2)(b)(ii)** whether disclosing the information could be reasonably expected to improve competition; and

The head must consider whether the disclosure will improve competition.

In considering the factors, **subsection (c)** states information the head must not use as a factor. It is the release of information to the public that is being considered, not the specific applicant.

> **82(c)** the head must not consider the following factors:
>
> **82(c)(i)** the applicant's identity or motive for requesting access to the information,
>
> **82(c)(ii)** whether the medium in which the information is available would, if the information were disclosed in that medium, contribute to misunderstanding of the information by the applicant or the public,

In considering the factors, the head must not use whether they believe the information could be misunderstood because the information is not clear, up-to-date or complete. The head can include an explanation if clarity is a concern rather than not releasing it.

> **82(c)(iii)** whether there are means, other than through submitting an access request, for the applicant or the public to become aware of the information or know that it exists.

In considering the factors, the head must not use whether there are other ways for the public to access the information.

Duty to disclose information under section 82

A public body has a duty to disclose information if **section 82** applies. If a complaint were made to the Information and Privacy Commissioner that a public body did not disclose information in the public interest, the public body would have to show why it did not do so in that particular situation.

Public bodies may find it helpful to plan for the release of information in emergency like situations by developing an assessment of the conditions under which section 82 might arise, the information that might be involved, and considerations that might be relevant to the decision-making process. It is recommended that a senior official in the public body, such as the head, retain the authority for decisions on section 82 disclosures.

SECTION 83 Duty to disclose if risk of significant harm

This provision is a general override for all other provisions of this act. It requires the head to disclose any information, including personal information, if they believe an individual or group of individuals will be at risk of significant harm. The head will disclose the information to the affected individual or group of individuals.

This provision applies to information that reveals a risk of significant harm to the general public, a specific group of people, or an individual, including an applicant.

"SIGNIFICANT HARM" means bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property, or any other similar types of harm.

The determination that there is a risk of harm to the environment or to public health or safety is usually made by professionals working for the public body or contracted by the public body to assess situations where there is a possible risk of harm. Determining the nature and extent of the risk is part of the management process. Since this provision refers to significant harm, the head of a public body must believe that the risk of harm is considerably greater than in normal circumstances.

HARM TO THE ENVIRONMENT refers to the damage to or degradation of any component of the earth, including air, land, and water; any layer of the atmosphere; and any organic and inorganic matter. Harm to the environment also includes damage to, or degradation of, the interacting natural systems that include components of these things, through either natural calamity or illegal or improper use. An example of a risk of significant harm to the environment might be information about toxic emissions from an industrial plant.

HARM TO HEALTH means damage to the well-being of the body or mind of an individual, or the health of the general public. An example of a risk of significant harm to health might be the presence of contaminants or a highly contagious virus in school buildings or contamination of a water supply.

HARM TO SAFETY means injury to the individual or to the collective condition of being free from danger or risk. A risk of significant harm to safety might be created by a natural gas leak or a bomb threat in a populated area.

An example is when a compelling risk to public health results in an order issued under the *Public Health and Safety Act*.

> **83(1)** Despite any other provision of this Act and in the absence of an access request, if the head of a public body determines that without disclosure of information (including personal information) held by the public body, an individual, a group of individuals or the public is, or is likely to be, at risk of significant harm, the head must, without delay after making the determination, disclose the information to the individual, the group of individuals or the public.
>
> **83(2)** Before, or if that is not practicable then as soon as practicable after, the head of a public body discloses information under subsection (1), the head must
>
> **83(2)(a)** provide, in accordance with the regulations, if any, and each applicable protocol, a notice of the disclosure to each individual who the head reasonably believes could be adversely affected by the disclosure; and

This provision requires the head to notify each person who could adversely be affected by disclosing the information, before the disclosure occurs or as soon as practicable.

Normally, notice must be given to affected third parties and the Information and Privacy Commissioner before the information is released. This obligation to notify third parties and the Commissioner must be balanced against the obligation to disclose the information without delay. Notification is to take place only where practicable, and the head of the public body must ensure that there is no delay adversely affecting the public interest. The factors governing release without delay apply here.

The third party notice should be sent to any person, group of persons or organization that is a subject of the information or the record(s), other than the person who made the request or the public body involved.

> **83(2)(b)** provide a copy of the notice to the commissioner.

This provision requires the head to notify the Commissioner, before the disclosure occurs or as soon as practicable. A similar notice, or a copy of the one sent to the affected person together

with a covering note, must be sent to the Commissioner to inform that office that a disclosure in the public interest is being made.

Public bodies that intend to disclose information in the public interest should not inappropriately disclose personal information of a third party. The amount and type of personal information that is disclosed should be limited to what is necessary to make the public or the affected group or individual sufficiently aware of the risk or danger to their health or safety or to the environment.