Freedom of Information and Protection of Privacy Act – Companion Document

1. Definitions

In this Act and any rules or forms made under it:

Access: the right to see information as explained in Section 18.

Access request: a request made under Section 21 to see information.

Applicant: a person who sends a written request to the Privacy Officer to see information.

Business day: any weekday, except a holiday.

Contact information: details that help you reach someone at their work, like their name, job title, phone number, address, email, or fax.

Canada: the Government of Canada.

Citizen: what the constitution says it means.

Collection: gathering or getting personal information. It does not include how the information is used, shared, or managed.

Consent: the right to give, refuse, or take back permission.

Constitution: the Constitution of the Kwanlin Dün First Nation (KDFN).

Council: what the constitution says it means.

Director: the leader of a department at KDFN, even if the department is not set up by law.

Elders Council: what the constitution says it means.

Employee: a person who works or volunteers for KDFN.

Executive Director (or their designate): the senior staff member leading the administration of KDFN.

Final agreement: the land claim agreement between KDFN, the Government of Canada, and the Government of Yukon that started on April 1, 2005.

Government: any public government, including KDFN.

Health Information Privacy and Management Act: is the Yukon law that protects people's health information and their right to access it.

Judicial Council: what the constitution says it means.

Identified person: the person the information is about, and who can be recognized from it.

Kwanlin Dün First Nation: what the constitution says it means.

Kwanlin Dün First Nation law: the constitution and any laws or rules made under it.

Law enforcement: policing, including criminal investigations; investigations or court actions that could lead to punishment or orders under Kwanlin Dün or Canadian/Yukon laws; or actions to make sure people follow the law.

Personal information: recorded details about a person that are not contact information.

Personal health information: what the Health Information Privacy and Management Act defines.

Privacy breach: stealing, losing, or using personal information without permission under this Act.

Privacy impact assessment: a review done by KDFN to check if a law, system, project, program, or activity follows Parts 2 and 3 of this Act.

Public body: a government department or agency in Canada, a province, a territory, a city, or a First Nation.

Privacy Officer: the person chosen by the Executive Director to handle privacy matters.

Public officer: any KDFN employee or officer, including the Chief and Councillors.

Qualifying person: means someone with a real and important interest in information held by KDFN.

Record: books, papers, maps, photos, letters, or any stored information, but not computer programs.

Self-government agreement: the self-government agreement made by KDFN, Canada, and Yukon, starting April 1, 2005.

Third-party: anyone involved in a request for information or correction except the person who made the request, or KDFN.

Yukon: the Yukon Territory as defined by the Yukon Act (Canada).

Youth Council: what the constitution says it means.

PART ONE: GENERAL PROVISIONS

Purpose of this Act

2. (1) The purpose of this Act is to help KDFN be responsible to its citizens and protect their privacy by:
   (a) Letting the public request access to certain records,
   (b) Letting people see and if necessary,ask to fix their own personal information,
   (c) Setting clear limits on when access to information can be denied,
   (d) Deciding how KDFN collects, uses, shares, and keeps personal information safe, and
   (e) Allowing decisions under this law to be reviewed.

   (2) This Act should be understood in a way that helps KDFN work quickly and well while keeping costs reasonable and meeting the Act's goals.

3. (1) This Act applies to records that KDFN keeps or controls, unless this section says otherwise.

(2) This Act does not cover information that is protected by the Health Information Privacy and Management Act (Yukon), except as described in subsection (3).

(3) Parts 30(1)(a) to (j) of this Act still apply, even if the Health Information Privacy and Management Act (Yukon) says something different.

(4) This Act does not stop:
- (a) people from getting information they are already allowed to have via existing public access, in court or other legal matters, and
- (b) KDFN from sharing general information (not personal) with the public if it chooses to.

(5) This Act does not apply to:
- (a) records used in court or decision-making hearings,
- (b) personal notes, messages, or draft decisions made by someone acting like a judge,
- (c) records held by an election officer during a vote or referendum,
- (d) meeting discussions of Council or Council committees when the public is not allowed to attend,
- (e) test or exam questions,
- (f) teaching or research materials from school staff,
- (g) records about a court case that isn't finished yet,
- (h) records that KDFN sells to the public,
- (i) records that have nothing to do with KDFN's work,
- (j) computer records that track how someone used a system, and
- (k) deleted electronic records that staff can no longer access.

(6) Except for a person's right to see and get a copy of their own personal information, Part 5 of this Act only applies to records that KDFN made or received on or after February 19, 2005.

Application

4. If this Act disagrees with another KDFN law, this Act is the one that applies—unless the other law clearly says it still applies even if it conflicts with this one.

Limitation of liability

5. No one can take legal action against KDFN, Council, or anyone working for them for:
   (a) sharing or not sharing a record (including personal information) if they were not acting in bad faith, or
   (b) not giving a required notice if they were not being careless.

Designation of Privacy Officer

6. (1) KDFN must choose an employee to be the Privacy Officer.
   (2) The Director of the Department of Governance can choose one employee to take on this role.

PART TWO: COLLECTION, PROTECTION AND RETENTION OF PERSONAL INFORMATION

Purpose for which personal information can be collected

7. KDFN can only collect personal information if:
   (a) a KDFN law allows it,
   (b) it is needed for law enforcement,
   (c) it is directly related to and needed for KDFN's work, programs, or services,
   (d) the person gives the information at a public event they choose to attend, or
   (e) the person agrees to the collection of their information.

How personal information is to be collected

8. (1) KDFN must collect personal information directly from the person it's about, unless:
   (a) the person agrees to another way, or a KDFN law allows it,

(b) the information is needed for medical treatment and the person can't give it or give permission,
(c) the information is needed to:
  (i) decide if someone should get an honour or award,
  (ii) deal with a case before the Judicial Council or other decision-maker,
  (iii) collect or pay money (like a fine or debt),
  (iv) help with law enforcement, or
  (v) prevent domestic violence if it's likely to happen,
(d) the information comes from Canada, Yukon, or another government, or
(e) asking the person directly might give wrong or misleading information, or hurt the purpose of collecting it.
(f) the information is needed for managing or ending an employee's job, or
(g) the information is needed for an investigation or legal case.

(2) KDFN must tell the person they are collecting information from:
  (a) Why it is being collected,
  (b) The legal reason for collecting it, and
  (c) Who can answer their questions.

(3) This does not apply if:
  (a) The information is related to law enforcement,
  (b) Following these steps would:
    (i) Lead to wrong information being collected, or
    (ii) Hurt the purpose of collecting it, or
  (c) One of the exceptions above applies.

(4) KDFN does not collect personal information for this Act if it receives information that is not related to its programs or activities, does nothing with it, and deletes it.

Accuracy of personal information

9. If KDFN has someone's personal information, it must try its best to make sure the information is correct and complete.

Right to request correction of personal information

10. (1) If someone thinks their personal information is wrong or missing something, they can write to the Privacy Officer and ask for a correction.

(2) They must include enough details to explain what's wrong and why.

(3) The Privacy Officer can ask more questions and ask for documents if needed to help make a decision.

(4) Within 15 business days, the Privacy Officer must tell the person if the change must be made or not—and give a reason if not.

(5) If no correction is made, a note must be added to the file saying a correction was asked for.

(6) If a correction is made, the Privacy Officer must tell anyone who got the wrong information in the past year.

Protection of personal information

11. KDFN must keep personal information safe. It must take reasonable steps to stop anyone from seeing, using, sharing, or throwing away the information without permission.

Unauthorized disclosure prohibited

12. KDFN staff who can access personal information are not allowed to share it unless the law allows it or the person it's about agrees.

Notification of unauthorized collection, use, and disclosure

13. If a KDFN staff member thinks personal information was collected, used, or shared without permission, they must tell the Privacy Officer right away and explain why.

Privacy breach notifications

14. (1) If personal information is shared or leaked by mistake, the Privacy Officer must tell the person affected as soon as possible:
    (a) if it could cause serious harm like:
        (i) identity theft,
        (ii) injury,
        (iii) embarrassment,
        (iv) damage to reputation or relationships,
        (v) losing a job or chance,
        (vi) losing money,
        (vii) a bad credit score, or
        (viii) losing or damaging property.

    (2) The Privacy Officer does not have to tell the person if it could seriously harm their health or safety, or someone else's.

    (3) If the Privacy Officer does tell the person, they must follow the proper steps.

PART THREE: USE AND DISCLOSURE OF PERSONAL INFORMATION

Use of personal information

15. (1) KDFN can use personal information only if:
    (a) it's used for the reason it was collected,
    (b) the person says it's okay,
    (c) it's contact information used to get in touch with a Beneficiary or Citizen,
    (d) it's used to check if someone can get or keep a program or benefit,
    (e) a lawyer needs it to help KDFN,
    (f) it's kept as part of KDFN's history (archives),

(g) it's used to plan or improve KDFN's work, and the information is made anonymous first,
(h) it's used to manage KDFN staff.

(2) KDFN can only use the information as much as needed to do its job properly.

Disclosure of personal information

16. (1) KDFN must only share personal information if this section allows it.

(2) KDFN can share personal information if:
(a) it follows the rules in Part Five,
(b) it's for the same reason the information was collected,
(c) the person agrees in writing,
(d) a law says it can be shared,
(e) an agreement made under KDFN law says it can be shared,
(f) a court or legal order requires it,
(g) a KDFN staff member needs it to do their job,
(h) it helps police or law enforcement,
(i) it helps collect or pay money owed,
(j) it protects someone's mental or physical health or safety,
(k) it helps contact a spouse, family member, or friend of someone who is hurt, sick, or has died,
(l) it's needed to check records,
(m) the person gave consent at a public event,
(n) it's needed to fix or maintain electronic systems, or recover data.
o) it's needed for an investigation or legal case involving KDFN.
p) it's needed to provide legal services to KDFN.

(3) Council may allow personal information to be shared for research or statistics if: it helps KDFN, there's no other way to do it, and the Council sets rules to protect the information.

(4) KDFN may also share personal information for historical purposes if:
(a) it doesn't unreasonably invade someone's privacy,
(b) it's used for research and meets the rules in subsection 3,
(c) the record is over 100 years old, or
(d) the person has been deceased for at least 20 years.

17. Personal information is being used properly if:
    (a) it's clearly connected to why it was collected, and
    (b) it's needed to do KDFN's work or run a legal program.

PART FOUR: PUBLIC INTEREST DISCLOSURE

Public interest disclosure obligations

18. (1) If there's a serious risk to the environment, health, or safety, KDFN must share the information right away—even if no one asked for it.

    (2) This must be done even if other parts of the law say something different.

    (3) Before sharing, the Privacy Officer must:
        (a) tell the person the information is about, if possible, or
        (b) send a letter to their last known address if they can't be reached.

PART FIVE: FREEDOM OF INFORMATION

Right of access to information

19. A Citizen or Beneficiary has the right to see and get a copy of their own personal information held by KDFN. But they can't see any parts that are protected under Sections 30 and 31.

20. (1) Citizens, Beneficiaries and other approved people can see and get copies of KDFN records. But some information is private under Sections 30, 31, and 32.

    (2) The Privacy Officer decides who counts as an approved person.

21. Beneficiaries and Citizens have the right to see a record, but:
    (a) if KDFN has an agreement with others, that agreement applies,
    (b) they can't see parts that are protected by law, but they can see the rest if those parts can be taken out,
    (c) some meeting records can be limited, even if they didn't attend the meeting,
    (d) they might have to pay a fee to get the record.

How to make an application

22. (1) To ask for a record, a person must write to the Privacy Officer with enough details to find it. If they are not a Citizen or Beneficiary, they must explain why they can ask.

(2) They can ask to see the record or get a copy.

(3) Someone can request another person's record if they have written permission from the person the record is about.

Power to disregard requests

23. (1) The Executive Director can let the Privacy Officer ignore a request if it would seriously disrupt KDFN's work because the request:
(a) is repeated many times, or
(b) is meant to bother or has no real purpose.

(2) This decision must be in writing, and the Privacy Officer must give a copy to the person who made the request.

Duty to assist applicants

24. (1) The Privacy Officer must:
(a) try their best to help people find the record they are looking for,
(b) reply to each request quickly, clearly, and honestly.

(2) The Privacy Officer must create a record if:
(a) it can be made using KDFN's usual computers and tools, and
(b) making it won't cause serious problems for KDFN's work.

Power to request information or fee

25. (1) Before accepting a request, the Privacy Officer can send a note to:
(a) ask for more information, or
(b) ask for payment of some or all of the fee.

(2) The time to respond is paused until the Privacy Officer gets what they asked for.

(3) The note must say that if the person doesn't reply in 30 business days, the request can be closed.

Abandoned applications

26. (1) If the applicant doesn't reply in time, the Privacy Officer can close the request.

(2) The applicant can ask the Judicial Council to look at that decision.

Time limit for response

27. The Privacy Officer must reply to a request within 30 business days, unless more time is allowed under section 28.

Extending the time limit for response

28. (1) The Privacy Officer can take up to 30 extra business days to reply if:
(a) there are too many records to go through in time, or
(b) they need to talk to someone else before deciding.

(2) If those problems continue, the Privacy Officer can take up to 45 more calendar days.

(3) If time is extended, the Privacy Officer must tell the person:
(a) why they need more time and when to expect a reply, and
(b) that the person can ask for the decision to be reviewed.

(4) If there's no reply in time, it counts as a refusal.

Contents of response

29. (1) The Privacy Officer's response must include:
(a) if the person can see the record or part of it,

(b) how they will get the record if allowed,
(c) if not allowed:
  (i) the reason why and what law supports it,
  (ii) who they can contact for questions, and
  (iii) that they can ask for the decision to be reviewed (Section 35).

(2) The Privacy Officer will not say if a record exists if:
(a) it has law enforcement information, or
(b) it includes someone else's private information and saying it exists would go against their privacy.

How access must given

30. (1) If a person can see a record, it must be given the right way.

(2) If they want a copy and it can be copied, they get a copy.

(3) If it can't be copied, they can either:
(a) look at it, or
(b) get access another way allowed by the rules.

Exceptions

31. (1) The Privacy Officer can refuse to share a record when it might:
(a) Harm private discussions or secrets of KDFN Councils or committees,
(b) Reveal confidential advice or plans,
(c) Expose law enforcement or investigation details,
(d) Break legal protections and expose security,
(e) Hurt KDFN's relationships with other governments,
(f) Reveal secret information from other governments,
(g) Damage KDFN's or its businesses' money or deals,
(h) Harm sacred sites, rare animals, or nature,
(i) Harm KDFN language, culture, or spirituality, or
(j) Put public safety or a person at risk.

32. (1) The Privacy Officer must refuse access to third-party business information when:
(a) The record contains secrets like trade, financial, or technical information from another business,

(b) That information was given in confidence, and
(c) Sharing it could seriously hurt that business, stop similar information being shared with KDFN, cause unfair money loss or gain, or reveal information from labor dispute reports.

(2) Subsection (1) does not apply if the third party agrees to the disclosure.

33. (1) The Privacy Officer must not give someone access to another person's personal information if it would unfairly invade that person's privacy.

(2) Sharing personal information is usually considered an unfair invasion of privacy if it includes:
(a) Medical or mental health history,
(b) Law investigations (unless needed for the case),
(c) Social assistance or benefits,
(d) Work or school history,
(e) Tax information,
(f) Personal finances or credit,
(g) Personal recommendations or references,
(h) Race, religion, sexual orientation, politics, or family history,
(i) Names with addresses or phone numbers for mailing or calls.

(3) Sharing personal information is not considered an unfair invasion of privacy if:
(a) The person agrees in writing
(b) It's needed for a health or safety emergency, and the person is notified
(c) A law allows it (from KDFN, Yukon, or Canada)
(d) It's used for approved research or statistics
(e) The person is a public officer, and the information is about their job or pay range
(f) The information is part of a contract with KDFN
(g) The information is about travel paid by KDFN
(h) The information is about a public license or permit—not personal application details
(i) The information is about a financial benefit—not personal application details

(4) Before deciding, the Privacy Officer must consider whether:
(a) The person would be unfairly harmed,
(b) The information might be wrong or unreliable,

(c) The information was given in confidence,
(d) Sharing could unfairly hurt someone's reputation,
(e) The information is needed to protect the applicant's rights,
(f) Sharing promotes openness about KDFN's activities,
(g) Sharing supports public health or safety.

Third party notice

34. (1) If the Privacy Officer thinks the record has private or sensitive information, they must:
(a) Tell the other person (third party) that someone asked for a record that may affect their privacy or business. The requester's name will not be shared.
(b) Give a short description of what's in the record.
(c) Let the third party know they have 20 business days to say yes to sharing or explain why it should stay private.

(2) The Privacy Officer must also tell the person who asked for the record:
(a) The record may include someone else's private or business information.
(b) The other person is being asked what they think.
(c) A decision must be made in 30 business days.

Time limit and notice of decision

35. (1) The Privacy Officer must decide within 30 business days if the applicant can see the record or part of it. But they must wait until:
(a) the third party replies, or
(b) 21 business days have passed—whichever comes first.

(2) Once the decision is made, the Privacy Officer must send a letter to:
(a) the person who asked for the record (the applicant), and
(b) the person the record is about (the third party).

(3) If the decision is to share the record, the letter must say it must shared—unless the third party asks for a review within 15 business days.

PART SIX: COMPLAINTS, RECONSIDERATIONS AND REVIEWS

Complaints

36. If a person believes the KDFN did not follow the rules in Parts 2, 3, 4, or 5, they can send a written complaint to the Privacy Officer. They must include any documents, written notes, or other information needed to help explain the complaint.

37. The Privacy Officer must review the complaint and can ask questions or accept more information before making a decision.

38. After reviewing the complaint, the Privacy Officer must send a written decision that either:
    (a) dismisses the complaint, or
    (b) accepts it fully or partly.
    The notice must also tell the person they can ask the Judicial Council to review the decision.

39. If the Privacy Officer accepts the complaint (in full or in part), they can require a public officer to fix or change the record, if needed.

40. The Privacy Officer cannot decide:
    (a) who is legally responsible, or
    (b) if anyone should be paid money.

Request for Reconsideration

41. A person who gets a decision from the Privacy Officer under Section 37 can ask the Judicial Council to review that decision. They must send the request within 15 business days and include a written statement explaining why, plus any documents or information needed.

42. When a request for review is made, the original decision is put on hold. But any actions taken before the review started are still valid.

43. The Judicial Council must send a copy of the review request to everyone who had a chance to give input on the original decision.

44. Anyone who gets a copy of the review request
    (a) can send their own comments about the request or the decision; and
    (b) must send their comments within 15 business days of getting the request.

45. The Judicial Council will look carefully at the review request. They can also consider earlier information or ask for more details before deciding.

46. The Judicial Council must make a decision within 40 business days of the Privacy Officer's original decision. But they cannot decide before:
    (a) they get a response from everyone who received the review request, or
    (b) 31 business days after the original decision notice was given—whichever comes first.

47. (1) After reviewing, the Judicial Council will send a written decision to the person who asked for the review, either agreeing with or changing the original decision.

    (2) A person cannot ask for a review unless they first tried any other administrative options available under this Act.

PART SEVEN: RECORDS MANAGEMENT

Establishment of records management system

48. The KDFN will set up and run a records management system to make sure all information it holds is handled following accepted Canadian records management standards.

Retention of information

49. If KDFN uses someone's personal information to make a decision about them, they must keep that information for at least one year.

PART EIGHT: ENFORCEMENT

Offences and penalties

50. (1) A person must not willfully:
    (a) make a false statement to, or try to mislead, the Privacy Officer or anyone else carrying out duties under this Act; or
    (b) block the Privacy Officer or anyone else from doing their duties under this Act.

    (2) A person who breaks subsection (1) commits an offence and can be fined up to $5,000, jailed for up to six months, or both.

PART NINE: PERIODIC REVIEW OF THIS ACT

Review report

51. By the date this Act starts and every year after, the Director of the Department of Governance must prepare a report for the Council on how the Act is working, including any recommendations to improve it.

Annual report of Privacy Officer

52. The Privacy Officer must provide a written annual report to the Executive Director of Governance that includes:
    (a) the activities of the Privacy Officer's office; and
    (b) any complaints or applications received under Part Six.

PART TEN: MISCELLANEOUS

Delivery and Notice

53. Delivery of any document or notice to a person must do in one of the following ways:
    (a) in person – counts right away.
    (b) by registered mail – sent to the person's provided or last known address. Counts 5 business days after sending.

(c) by email – if the person agrees or confirms they got it. Counts when they confirm or 2 days after sending, whichever is first.

Regulations

54. The Council may make rules to help carry out this Act. These rules can cover things like:
    (a) when people can look at records (business hours);
    (b) how to give access to records and keep personal information safe;
    (c) how and when to notify third parties (like in section 28(2));
    (d) steps and timelines for handling record requests and protecting personal information;
    (e) how to safely destroy records;
    (f) types of records and how to make them public;
    (g) limits on viewing records to protect personal information;
    (h) fees for copies or services;
    (i) how to handle complaints or review requests; and
    (j) any other rules needed to make this Act work properly.

Act in force

55. This Act will take effect on a date, or different dates, set by the Council.