

<b>Statement of Policy and Procedure</b>	
<b>Policy No.</b>	<b>Information Management Policy</b>
<b>Department Ownership</b>	<b>Administration</b>
<b>Issue/Effective Date</b>	<b>March 7, 2019</b>
<b>Policy Number</b>	<b>GFN2019/002</b>
<b>Amendment Record</b> <i>(Record the date here and attach Council BCR for each Amendment)</i>	

**Glooscap First Nation**

**Information Management Policy**

## Table of Contents

<b>1. Definitions</b>	4
<b>2. Information Technology</b>	6
A. Policy .....	6
B. Purpose .....	6
C. Scope .....	6
D. Responsibilities .....	6
E. Procedures .....	6
(1) Planning and Evaluation .....	6
(2) Outsourcing .....	7
(3) Data Management .....	7
(4) Access Management .....	7
(5) Information System Security .....	8
(6) Change Management .....	8
(7) Monitoring .....	9
F. References and Related Authorities .....	9
G. Appendices .....	10
<b>3. Record Information Management</b>	11
A. Policy .....	11
B. Purpose .....	11
C. Scope .....	11
D. Responsibilities.....	11
E. Procedures .....	12
(1) Accountability .....	12
(2) Creation and Collection .....	12
(3) Organization and Classification .....	13
(4) Maintenance, Protection and Preservation .....	13
(5) Retention and Disposition .....	14
F. Reference and Related Authorities .....	14
G. Appendices .....	14
<b>4. Information Privacy</b>	15
A. Policy .....	15
B. Purpose .....	15
C. Scope .....	15
D. Responsibilities .....	15
E. Procedures .....	16
(1) Accountability .....	16
(2) Identifying Purpose .....	16
(3) Consent .....	17
(4) Limiting Collection .....	18
(5) Limiting Use, Disclosure and Retention .....	18
(6) Accuracy .....	18

(7) Safeguards .....	18
(8) Openness .....	19
(9) Individual Access .....	19
(10) Challenging Compliance .....	20
F. Reference and Related Authorities .....	20
G. Appendices .....	20
<b>5. Departmental Records Management</b>	<b>21</b>
A. Policy .....	21
B. Purpose .....	21
C. Scope .....	21
D. Responsibilities .....	21
E. Procedures .....	21
(1) Collection of Records .....	21
(2) Human Resource Files .....	22
(3) Social Assistance Files .....	22
(4) Native Employment Files .....	22
(5) Membership Files .....	23
(6) Education Files .....	23
(7) Council Records .....	24
(8) Housing and Tenancy Files .....	24
(9) Health and Medical Records .....	25
F. References and Related Authorities .....	26
G. Appendices .....	26
<b>6. Complaints and Appeals Policy</b>	<b>27</b>
A. Policy .....	27
B. Purpose .....	27
C. Scope .....	27
D. Responsibilities .....	27
E. Procedures .....	27
F. References and Related Authorities .....	28
G. Appendices .....	28

**List of Appendices**

- A. Glooscap First Nation Server Backup Check Sheet for Cartridge Change
- B. Glooscap First Nation Document Retention Periods
- C. Glooscap First Nation Document Disposition Form
- D. Glooscap First Nation Records Management Permissions Tracking Spreadsheet
- E. Glooscap First Nation Privacy Statement
- F. Glooscap First Nation Breach of Privacy Complaints Form

## 1. Definitions

<b>“Classification”</b>	is the process of categorising records according to a predetermined hierarchy or scheme. Functional-based classification is the arrangement of records based on the business functions and activities of Glooscap First Nation. This allows the Council to understand the records collected and created related to each business process / activity and how that record is used.
<b>“Director of Administration”</b>	means the person who is responsible for leading the day to day administration or management of Glooscap First Nation and who reports directly to Council. The Senior Manager, as defined in the Glooscap First Nation Financial Administration Law is the same as the Director of Administration.
<b>“Information”</b>	is knowledge communicated or received and may be any documentary material regardless of communications source, information format, production mode or recording medium.
<b>“Information Security”</b>	refers to the physical, electronic and policy instruments that are used to protect information from unauthorized access (protecting confidentiality), unauthorized use (protecting integrity), unauthorized modification (also protecting integrity) and unauthorized destruction (protecting availability).
<b>“Officers”</b>	means the Senior Manager, Senior Financial Officer, Tax Administrator or any other employee of Glooscap First Nation designated by the Council as an Officer;
<b>“Personal information”</b>	refers to all information that reveals factual or subjective elements of knowledge about an identifiable individual. In addition to the basic elements that are commonly used to identify and interact with an individual - such as the individual’s name, gender, physical characteristics, address, contact information and identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of the individual’s life.
<b>“Privacy Protection”</b>	refers to the decisions made by a First Nation in regards to the acceptable ways to collect, create, use, share/disclose,

retain, protect and dispose of the Personal Information that it needs for its administrative and operational needs.

**“Record”**

is a special form of information, and for the purposes of this policy refers to information created, received, and maintained by Glooscap First Nation for business purposes or legal obligations, which enable and document decision-making, and support First Nation reporting, performance and accountability requirements. A record may be electronic or hardcopy paper based.

**“Recordkeeping”**

is a framework of accountability and stewardship in which records are created or acquired, captured, and managed as a vital business asset and knowledge resource to support effective decision-making and achievement of results for Glooscap First Nation.

**“Repository”**

refers to a preservation environment for a record. It includes specified physical or electronic storage space and the associated infrastructure required for its maintenance. Business rules for the management of records in a Repository need to be established, and there must be sufficient control for the resources to be authentic, reliable, accessible and usable on a continuing basis.

**“Rollback Procedure”**

means the ability to restore system to previous configuration prior to change, with documented procedures and steps to complete the process.

**“Virtual Private Network”**

means a Virtual Private Network (“VPN”) which is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

## **2. Information Technology**

### **A. Policy**

Glooscap First Nation's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect Glooscap First Nation's information.

### **B. Purpose**

The purpose of this policy is to ensure that information system integrity, specifically as it relates to the financial administration system, is maintained and supports the strategic and operational requirements of Glooscap First Nation.

### **C. Scope**

This policy applies to all employees involved in the selection, implementation, operations, or ongoing maintenance of Glooscap First Nation's information systems. This includes the Senior Manager, and information technology employees.

### **D. Responsibilities**

- (1) Council is responsible for:
  - a. Approving the establishment and implementation of documented procedures for information technology used by Glooscap First Nation in its operations.
- (2) The Senior Manager is responsible for:
  - a. Ensuring that controls are in place over information technology, whether performed by an internal employee or outsourced to an external organization;
  - b. Monitoring the performance of internal and/or external information technology professionals.
- (3) The information technology professional is responsible for:
  - a. Maintaining the integrity of information systems within Glooscap First Nation.

### **E. Procedures**

- (1) Planning and evaluation
  - a. The Council, with the assistance of the Senior Manager and input from information technology employees, will ensure that information systems are developed that support Glooscap First Nation's strategic plan and operations.
  - b. When there are no individuals internally with the requisite technical skills to identify information technology requirements or evaluate options, the Senior Manager will seek advice from a qualified external individual or organization.

(2) Outsourcing

- a. Subject to the Procurement Policy, the Senior Manager is responsible for the selection of contractors providing information technology services, the definition of services in their contracts, establishing service level agreements and the administration of the contracts.
- b. Specific items which should be included in the procurement of information technology services and final contract with the chosen provider include:
  - i. A requirement that the service provider submits regular reports of all work performed on Glooscap First Nation's information systems;
  - ii. A requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information;
  - iii. Access by outsourced parties to First Nation information is provided on a 'need to know basis' only.

(3) Data management

- a. Subject to the Records and Information Policy, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.
- b. All sensitive, valuable, or critical information/data residing on Glooscap First Nation's information technology systems must be periodically backed-up. Backups will occur incrementally on a daily basis, with full backups on a weekly and monthly basis.
- c. Backup drives must be stored in a secure location with access limited to the Senior Manager and limited other employees as appropriate. Ideally, backup drives will be securely stored at an offsite location that is easily accessible to individuals with authorized access.
- d. Backup drives will be retained for a period of 3 months before being overwritten or deleted.

(4) Access management

- a. All individuals requiring access to First Nation information systems will have unique user identification. Shared user IDs or passwords will not be permitted, with the exception of the finance department.
- b. Requests for access to Glooscap First Nation's network, accounting system, or other access restricted information system must include a description of an employee's role and rationale for the level of access required. Signed approval must be obtained from the Senior Manager (or designate).

- c. User ID and password are required for access to the network and other critical programs/areas such as the accounting system. Automatic authentication using scripts or macros inserting user IDs and/or passwords are prohibited.
- d. Individuals will be given access privileges to the extent necessary to fulfill their individual job function and no more. Systems and applications should not be configured with unrestricted access to all data.
- e. When an individual or contractor is terminated or ends employment with Glooscap First Nation, their user IDs must be disabled immediately.
- f. Support personnel must notify the user when attempting to take control of a workstation. All instances where specific software is loaded to remotely control a workstation must be removed when the support function is completed. The use of the remote-control software must be in accordance to applicable agreements.

(5) Information system security

- a. Security tools and techniques are implemented to enable restrictions on access to programs and data.
- b. Security tools and techniques are administered to restrict access to programs and data.
- c. Each computer resource must have an approved antivirus program installed. The following standards must be met:
  - i. The antivirus program must not be disabled and must be configured to scan all programs and files upon execution and must have real time protection enabled. If encrypted and password protected files cannot be virus checked, it is the responsibility of the user to ensure that virus checking takes place whenever this protection is removed;
  - ii. Antivirus files must be updated on the network every two weeks or whenever a new threat is identified.
- d. Network firewalls must be configured to support a 'least-privilege' approach to security, allowing only specific systems, services and protocols to communicate through the network perimeter. Logical and physical access to these systems must be limited strictly to those personnel with specific training and authorization to manage the device. Additionally, the following Firewall standards must be addressed:
  - i. Firewall and proxy servers must be securely installed;
  - ii. Detailed firewall logs must be maintained;
  - iii. Alerts must be raised if important services or processes crash.

(6) Change management

- a. All new data structure and modifications to data structure will be tested before implementation.
- b. All computers, hardware, software and communication systems used for a production environment must employ a documented change control process. The change management process should include the following activities:
  - i. The data structure is consistent with the needs of Glooscap First Nation;
  - ii. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent the needs of Glooscap First Nation;
  - iii. An assessment of any risks involved with the change;
  - iv. Implementation considerations;
  - v. A description of the testing required;
  - vi. Approval from the Senior Manager;
  - vii. Communication of changes to First Nation employees as appropriate.

(7) Monitoring

- a. Only approved and authorized programs will be implemented onto First Nation information management systems. Periodic reviews of the workstations and the system will take place to monitor compliance with this requirement.
- b. A log of employees, their user IDs, and their access levels within First Nation information systems will be maintained. On a quarterly basis, the Senior Manager will review the log to ensure users and the associated access rights are appropriate. Access rights that will be monitored include the following:
  - i. User access management (i.e. the accounting system);
  - ii. Third party access (i.e. outsourced information technology professionals);
  - iii. Network access and file sharing;
  - iv. Remote and VPN access.
- c. Network system performance is monitored on a regular basis.
- d. The firewalls must be monitored daily and their functionality audited semi-annually.

**F. References and Related Authorities**

- (1) FMB's Financial Management System Standards
  - a. Standard 19.8 - Information Technology Controls
- (2) FMB's Financial Administration Law Standards
  - a. Standard 17.6.2 - Information Technology Controls

## **G. Appendices**

(1) Appendix A – Glooscap First Nation Server Backup Check Sheet for Cartridge Change

### **3. Record Information Management**

#### **A. Policy**

Records are a special form of information that are created, received, and maintained by Glooscap First Nation for business purposes or legal obligations, which enable and document decision-making, and support First Nation reporting, performance and accountability requirements. Records must be created and collected, organized, retained, and safeguarded in a manner that enables their long-term availability, understandability and usability.

#### **B. Purpose**

The purpose of the policy is to provide guidance on effective recordkeeping practices that enable Glooscap First Nation to create and acquire; manage; and, protect the integrity of its records that support its decision-making, and support First Nation reporting, performance and accountability requirements.

#### **C. Scope**

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of Glooscap First Nation and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all records created and acquired by Glooscap First Nation regardless of format (i.e., both electronic and hardcopy paper records).

#### **D. Responsibilities**

- (1) Council is responsible for:
  - a. Approving the establishment and implementation of documented procedures for records management within Glooscap First Nation.
- (2) The Senior Manager is responsible for:
  - a. Implementing appropriate recordkeeping practices,
  - b. Ensure appropriate safeguards of Glooscap First Nation's records;
  - c. Ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process;
  - d. Ensuring that employees and any contractors or volunteers performing services on behalf of the Council are fully knowledgeable of their responsibilities as they relate to recordkeeping practices.
- (3) Employees, contractors and volunteers are responsible for:
  - a. Complying with the established records management policy.

- b. Immediately reporting to their supervisor any potential breach related to compliance with the record keeping policy, including the incidents in which the safeguarding of records may have been compromised.

## **E. Procedures**

### **(1) Accountability**

- a. Each record shall have a designated steward that ensures the recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, or volunteer that are in custody of a record must ensure it is managed in accordance with this policy.
- b. Permanent records such as operations manuals, policies, and procedures will be reviewed and updated by the steward periodically, but at least every two years, or more frequently as required.
- c. Records under the stewardship of an employee or any contractor or volunteers that is departing must be formally transferred to another employee through a knowledge transfer process. This process should include information on the types of records to be transferred, how the records are organized, in which repository the records are kept, and required safeguards.

### **(2) Creation and Collection**

- a. All important activities and decision-making processes of Glooscap First Nation should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect Glooscap First Nation from liability.
- b. All information at its time of creation or collection should be assessed to determine if it supports Council's business purposes or legal obligations and enables decision-making. If determined to be a record its management should comply with the procedures outlined within this policy.
- c. Glooscap First Nation's records shall be created using the most appropriate application so as to ensure that they adequately support the objectives for which they are created and can easily be used by those who need them to perform their duties – i.e., using MS Excel instead of MS Word to develop spreadsheets with financial figures, etc.
- d. Glooscap First Nation's records shall contain all the information which is necessary to achieve the objectives for which each of them is created; yet their contents shall be limited to only what is necessary to achieve those objectives. This should include limiting the information collected through forms to only that which is required.

- e. Whenever possible, the record shall contain information about one single function or activity so as to facilitate information Classification, organization, retention and retrieval.
- f. Glooscap First Nation's records shall be legible, written in plain language and adapted to their specific audience.
- g. Only one copy of each record should be created or collected. When creating or collecting a record, individuals should first check to see if the record is already in existence. In instances of multiple copies of the same record, copies should be securely disposed in accordance with the requirements of this policy.

### (3) Organization and Classification

- a. A classification plan structure shall be implemented based on Glooscap First Nations functions and activities, with records stored in accordance with the activity and/or function that it supports. This classification plan should be used to support the filing system for both electronic records and hardcopy paper-based records.
- b. Records should be subject to a consistent naming convention, with the name of the record including the title, date and version. Naming convention is GFNDocument\_Jan2019\_Final
- c. The title of the document should be short but meaningful.
- d. The title may contain multiple words and should be ordered from most specific to less specific related to the business activity or function.
- e. Common words such as 'draft' or 'letter' should not be at the start of the title.
- f. An official repository shall be identified and designated for each record, in which the record must be stored. The number of record repositories should be limited and be consistent to support the format and type of record.
- g. Records should be made accessible, shared and re-used to the greatest extent possible, subject to technological, legal policy and security restrictions.

### (4) Maintenance, Protection and Preservation

- a. Records must be protected and stored in the appropriate repositories in a way that preserves their long-term availability, understandability and usability.
- b. Backups should be taken of all electronic records on a regular basis and stored in a physical location separate from the location of the original records.
- c. Any records that are only in hardcopy paper-based format should be assessed to determine if they need to be scanned or if other physical security measures need to be taken (e.g. use of fire/water proof cabinets) to ensure their long-term availability.

- d. Records that contain personal information or information of a confidential nature related to the Council, or a third party, such as the confidential financial information related to a business, should be labelled as CONFIDENTIAL.
- e. Confidential records should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:
  - i. For electronic records, confidential records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Confidential records should not be emailed 'in the clear' without appropriate protection.
  - ii. For hardcopy paper-based records, confidential records should be stored in secure filing cabinets at all times unless being used and transported in a secure manner if required to be offsite.

(5) Retention and Disposition

- a. Glooscap First Nation records shall be retained for the period specified in the records and information retention and disposition schedule, as outlined in Appendix B. They shall be disposed of in a manner that prevents their reconstruction (for paper-based records) or recovery (for electronic records).

**F. References and Related Authorities**

- (1) The FMB's Financial Management System Standards
  - a. Standard 19.0 - Risk Management
  - b. Standard 23.0 - Records and Information
- (2) The FMB's Financial Administration Law Standards
  - a. Standard 21.0 - Records and Information

**G. Appendices**

- (1) Appendix B – Glooscap First Nation Document Retention Periods
- (2) Appendix C – Glooscap First Nation Document Disposition Form

## **4. Information Privacy**

### **A. Policy**

Ensuring the privacy of personal information provided to Glooscap First Nation by individuals is essential to not only ensure compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or substantially similar provincial legislation, but also to ensure continued stakeholder confidence in Glooscap First Nation and that accountability is maintained.

### **B. Purpose**

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within Glooscap First Nation related to the collection, use, disclosure, retention, and safeguarding of personal information.

### **C. Scope**

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of Glooscap First Nation and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all Personal Information created and acquired by Glooscap First Nation regardless of format (i.e., both electronic and hardcopy paper records).

### **D. Responsibilities**

- (1) Council is responsible for:
  - a. Establishing and implementing documented procedures for privacy and the management of personal information within Glooscap First Nation; and
  - b. Appointing a Privacy Officer to manage and oversee Glooscap First Nation's compliance with privacy requirements; and this policy.
- (2) The Senior Manager is responsible for:
  - a. Ensuring compliance with the established information privacy policy.
- (3) The Privacy Officer is responsible for:
  - a. Developing and maintaining standards, policies and procedures that support the objectives of Glooscap First Nation's privacy program;
  - b. Ensuring that all the activities of Glooscap First Nation are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the Privacy Officer will:

- i. Provide training and awareness on privacy protection.
  - ii. Ensure that community members are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the personal information which is kept about them by Glooscap First Nation.
  - iii. Act as an expert resource on privacy matters within Glooscap First Nation.
  - iv. Conduct periodic reviews of Glooscap First Nation's activities that involve the collection, use, disclosure, retention, and safeguarding of personal information.
- c. Investigating all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of Personal Information and reporting the results to the appropriate managers and, where warranted, to Council;
  - d. Recommending changes to policies, procedures and practices in response to the issues raised in the complaints; and
  - e. Responding in writing to the requests for access to, and correction of Personal Information submitted by employees and community members within thirty calendar days from the date of the receipt.
- (4) Employees, contractors and volunteers are responsible for:
- a. Complying with the established information privacy policy; and
  - b. Immediately reporting to their supervisor privacy breaches of which they become aware.

## **E. Procedures**

### **(1) Accountability**

- a. Glooscap First Nation must appoint a Privacy Officer to ensure the principles outlined in this policy are appropriately implemented.
- b. Glooscap First Nation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

### **(2) Identifying Purpose**

- a. The purposes for the collection of personal information should be communicated to individuals at or before the time of collection. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

- b. Personal information should be collected directly from the individual whenever possible.
- c. Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected.

(3) Consent

- a. With limited exceptions, Glooscap First Nation must obtain consent from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be subsequently used and disclosed.
- b. Consent must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent must not be obtained through deception.
- c. Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances. For example, legal or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Consent may be sought from an individual's authorized representative in certain cases, for example, when an individual is seriously ill, mentally incapacitated, a minor, or has died.
- d. If personal information is intended to be used or disclosed for a new purpose not identified during the original collection, and not related to the original purpose of the collection, the consent of the individual must be obtained.
- e. Individuals can give consent in many ways. For example:
  - i. a form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
  - ii. consent may be given orally; or,
  - iii. consent may be given through electronic means.
- f. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Glooscap First Nation must stop using the individual's personal information within a reasonable time period and inform the individual of this time period and the implications of such withdrawal.

#### (4) Limiting Collection

- a. Glooscap First Nation cannot collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

#### (5) Limiting Use, Disclosure and Retention

- a. Glooscap First Nation may only use or disclose personal information for the purpose for which it was collected, unless:
  - i. The use or disclosure of the personal information is consistent with the original collection of the personal information;
  - ii. The consent of the individual is obtained; or,
  - iii. It is for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.
- b. Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.
- c. Identifiable personal information must only be used and disclosed if required. For instance, consider if reports, research, or audits/assessments can be done through de-identified or anonymous data.
- d. Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with Glooscap First Nation's retention and disposition schedule.

#### (6) Accuracy

- a. Glooscap First Nation shall take all reasonable steps to ensure that personal information that is used to make a decision on an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

#### (7) Safeguards

- a. Personal information should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:
  - i. For electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Personal information should not be emailed 'in the clear' without appropriate protection.

- ii. For hardcopy paper-based records, containing personal information, the records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be taken offsite.
- b. Glooscap First Nation must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.
- c. Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

(8) Openness

- a. Glooscap First Nation must be open about its policies and practices with respect to the management of personal information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable.
- b. The information made available should include:
  - i. the name or title, and the address, of the Privacy Officer, who is accountable for Glooscap First Nation's policies and practices, and to whom complaints or inquiries can be forwarded;
  - ii. the means of gaining access to personal information held by Glooscap First Nation; and,
  - iii. a description of the type of personal information held by First Nation, including a general account of its use.

(9) Individual Access

- a. When requested, an individual must be informed if Glooscap First Nation holds personal information about the individual and provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
- b. The identity of an individual must be authenticated before discussing their personal information with them.
- c. When requested, Glooscap First Nation must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable.
- d. Individuals who are given access to their personal information may:
  - i. request correction of the personal information where the individual believes there is an error or omission therein;
  - ii. require that a notation be attached to the information reflecting any correction requested but not made; and,

- iii. require that any person or body to whom that information has been disclosed for use for a decision-making process within two years prior to the time a correction is requested, or a notation be notified of the correction or notation.
- e. In certain situations, Glooscap First Nation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that:
  - i. is prohibitively costly to provide;
  - ii. contains references to other individuals;
  - iii. cannot be disclosed for legal, security, or commercial proprietary reasons; or,
  - iv. is subject to solicitor-client or litigation privilege.

(10) Challenging Compliance

- a. Glooscap First Nation must ensure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.
- b. Glooscap First Nation must investigate all complaints. If a complaint is found to be justified, Glooscap First Nation will take appropriate measures, including, if necessary, amending its policies and practices.

**F. References and Related Authorities**

- (1) FMB's Financial Management System Standards
  - a. Standard 12.6 - Human Resource records
  - b. Standard 19.0 - Risk Management
  - c. Standard 23.0 - Records and Information
- (2) FMB's Financial Administration Law Standards
  - a. Standard 21.0 - Records and Information

**G. Appendices**

None

## **5. Departmental Records Management**

### **A. Policy**

Glooscap First Nation recognizes the varied programs and services provided by the Council and employees and the unique information management practices that may accompany each individual program.

### **B. Purpose**

The Departmental Records Management Policy outlines the procedures for the collection, retention, and disposal of program specific records in accordance with rules governing those programs.

### **C. Scope**

The policy applies to all members of Council, employees, volunteers, contractors or anyone working with Glooscap First Nation or any of its entities and who may be involved in the collection of personal or sensitive corporate information.

### **D. Responsibilities**

(1) Council is responsible for:

- a. Approving the establishment and implementation of the documented procedures for departmental records management used by Glooscap First Nation in its operations.

(2) The Director of Administration is responsible for:

- a. Ensuring that the employees are aware of and adhere to the procedures outlined in this policy.

(3) The Privacy Officer is responsible for:

- a. Responding to inquiries from employees in relation to proper records management.

### **E. Procedures**

(1) Collection of Records

- a. Glooscap First Nation collects personal information for a number of reasons including:
  - i. Human Resource files for Glooscap First Nation employees;
  - ii. Social Assistance Files;
  - iii. Work/Employment files as they pertain to the Native Employment program;
  - iv. Membership files of the registered members of Glooscap First Nation;

- v. Requests for Assistance;
- vi. Health and medical files through the Health and Healing Centre.
- b. The Glooscap First Nation Privacy Statement will be posted in all public buildings.
- c. A Permissions Tracking spreadsheet will be maintained by the Director of Administration to understand who is permitted to access files. The Permissions Tracking spreadsheet will document permissions for both paper and electronic files.

(2) Human Resource Files

- a. The procedures for Human Resource files are outlined in the Glooscap First Nation Human Resource Policy.

(3) Social Assistance Files

- a. The social assistance files will be created and maintained by the Social Development Officer and include (but not limited to) the following:
  - i. Name
  - ii. Contact Information
  - iii. Expression of need of social assistance (i.e. applications, proof of income, dependents etc.);
  - iv. Assessments and reports;
  - v. Change in status.
- b. Access to the Social Assistance files is restricted to the Social Development Officer. In some instances, the Director of Administration or the Senior Finance Officer may need to access the client's files. In such instances, the Social Development Officer will be present and return the files, safeguarding the privacy of the client.
- c. All social assistance files will be kept in a locked filing cabinet in the social development Officers office. When absent from the office, the door must be securely locked.
- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in a social assistance file will not be shared by outside sources (with the exception of Indigenous Services Canada) unless specified by law or with the written approval of the client.
- f. The information contained in the social assistance files is used to accurately understand the need of assistance of social assistance clients as well as general reporting to Indigenous Services Canada.

(4) Native Employment Files

- a. The Native Employment files will be created and maintained by the Native Employment Officer. The files must include but are not limited to:
  - i. Resumes (address, past work experience etc.);
  - ii. Copies of educational certificates;

- iii. Personal information (i.e. social insurance numbers, address, telephone number etc.)
- b. Access to the native employment files is restricted to the Native Employment Officer's office in accordance with the Mi'kmaq Employment and Training Secretariat (METS) sub agreement.
- c. All native employment files will be kept in a locked filing cabinet in the Native Employment Officers office. When absent from the office, the door must be securely locked.
- d. Personal information contained in an individual's native employment files will not be shared with outside sources (with the exception of funders) unless specified by law or with the written approval of the client.
- e. The information contained in the files is used to assist clients in finding employment and training opportunities as well as reporting to funders.

#### (5) Membership Files

- a. Membership files of Glooscap First Nation members include but are not necessarily limited to:
  - i. The Band list as provided by Indigenous Services Canada (ISC) or the Registry Clerk with the Confederacy of Mainland Mi'kmaq (CMM).
  - ii. Membership requests for assistance;
  - iii. Requests to forfeit membership;
  - iv. Files on custom adoption;
  - v. Estates and wills where requested by Band Members.
- b. Access to the membership files is restricted to the Director of Administration. In some instances, the Council may need to access a member's files. In such instances, the Director of Administration will be present, and the files will not leave the office of the Director of Administration.
- c. All membership files will be kept in a locked filing cabinet in the Director of Administrations office. When absent from the office, the door or the filing cabinet must be securely locker.
- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in the membership files will not be shared with outside sources (with the exception of government agencies with whom Glooscap First Nation has signed an agreement permitting them access) unless specified by law or with the written approval of the member.
- f. The information contained in the membership files is used to track membership levels, entitlement to compensation from gaming revenues, information sharing from Band to members etc.

#### (6) Education Files

- a. Education files will be created by the Education Officer. Education records include but are not limited to:
  - i. Name and address of student
  - ii. Records on attendance (i.e. what school they are currently attending, attended in the past etc.)
  - iii. Copies of applications for schools, grades, funding, scholarships etc.
- b. Access to the education files is restricted to the Education Officer. In some instances, the Director of Administration, the Senior Finance Officer, or the Council may need access to an individual's files but every effort should be made to minimize this.
- c. All education files are to be kept in a locked filing cabinet in the Education Officers office.
- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in the education files will not be shared with outside sources (with the exception of funders) unless specified in law or with the written consent of the client.
- f. The information collected in the education files is used to track school attendance at the elementary, secondary and post-secondary level for members of Glooscap First Nation, to provide information to funders to assist students in scholastic endeavours.

(7) Council Records

- a. Council records will be developed and maintained by the Director of Administration and include but are not limited to:
  - i. Council meeting minutes;
  - ii. Band Council Resolutions;
  - iii. Membership Requests for Assistance;
  - iv. Contracts;
  - v. Agreements with federal, provincial and municipal governments etc.
- b. Access to the Council files is determined on a case by case basis by the Director of Administration, in cooperation with Council.
- c. All Council records will be kept in a locked filing cabinet.
- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in the Council files (i.e. specific requests for assistance) will not be shared with outside sources (with the exception of funders) unless specified by law or with the written permission of Council.
- f. The information collected in the Council files is designed to maintain a record of Council business and decisions.

(8) Housing and Tenancy Files

- a. Housing and tenancy files will be created and maintained by the Housing and Infrastructure Officer. The Housing files include but are not limited to:

- i. Applications for Housing (includes personal information such as salary, marital status, disability status, criminal record check, credit check etc.)
  - ii. Maintenance requirements for homes;
  - iii. Lease agreements with tenants;
  - iv. Funding information from funders including but not limited to Indigenous Services Canada (ISC) and Canada Housing and Mortgage Corporation (CMHC).
- b. Access to the Housing files is restricted to the Housing and Maintenance Officer. In some occasions, the Director of Administration, Senior Finance Officer or the Council as a whole may need access to an individual's file but every effort should be made to minimize this.
- c. All housing files will be kept in a locked filing cabinet in the office of the Housing and Infrastructure Officer.
- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in the Housing and Tenancy files will not be shared with outside sources (with the exception of funders) unless specified by law or with the written approval of the client.
- f. The information collected in the housing files is used to track the tenancy of houses on Glooscap First Nation, the maintenance requirements of housing as well as the financial documentation of funders.

(9) Health and Medical Files

- a. Health and medical files will be created and maintained by the Community Health Nurse and the Health Director when required. The health and medical files include but are not limited to the following:
  - i. Name
  - ii. Demographic profile
  - iii. Contact Information
  - iv. Emergency Contact
  - v. Family Physician;
  - vi. Medical history;
  - vii. Medications being taken;
  - viii. Specific medical information (i.e. blood pressure, sugar levels, test results etc.)
- b. Access to the health and medical files is restricted to the Community Health Nurse. In some instances, the Health Director may need to access an individual's files but every effort should be made to minimize this.
- c. All health and medical files are to be kept in a secure room within the health centre. The file room must be locked at all times. Keys are provided to the Community Health Nurse and Health Director only.

- d. In adherence to the Glooscap First Nation Information Management Policy, any electronic files must be secured using passwords to ensure privacy is maintained.
- e. Personal information contained in the health or medical files will not be shared with outside sources (with the exception of a client's medical team or in the case of a medical emergency where the client is unable to provide consent) unless specified by law or with the written approval of the client.
- f. Information may be provided to funders in anonymized form for data collection purposes only.
- g. In the case of Assisted Living clients, records will be shared between the Community Health Nurse, Health Directors, Social Assistance Coordinator, and health care practitioner providing services.
- h. The information collected in the health and medical files are used to track the overall health and wellbeing of the clients, develop individualized programming and in the case of emergency, to provide medical professionals with necessary information for treatment.

**F. References and Related Authorities**

None

**G. Appendices**

- (1) Appendix D – Glooscap First Nation Records Management Permissions Tracking Spreadsheet
- (2) Appendix E – Glooscap First Nation Privacy Statement

## **6. Complaints and Appeals Policy**

### **A. Policy**

Council understands that employees and clients have the right to understand how their information is being used and to protect their personal information from unnecessary disclosure. Employees and clients need to have a means to ensure that their information has not been misused in any way.

### **B. Purpose**

The purpose of the policy is to outline procedures in the event that an employee, member, clients etc. feels that their personal information has been compromised and not collected and used with the intent outlined in the above policies.

### **C. Scope**

This policy applies to all members of Council, employees, clients, members, etc.

### **D. Responsibilities**

- (1) Council is responsible for:
  - a. approving the procedures laid out in this policy to ensure that employees, clients, members etc. have a means to hold those who collect information to account and ensure the safety of their own information.
  
- (2) The Director of Administration is responsible for:
  - a. Initiating any appeal or investigation into any perceived violations of this policy;
  - b. Reporting to Council on the result of the investigation;
  - c. Communicating with results of the investigation to the appellant;
  - d. Ensuring any actions derived from the investigation are completed.

### **E. Procedures**

- (1) Appeals Procedure
  - a. The party to the complaint has thirty (30) business days after they believe their information has been compromised to file a complaint, in writing, to the Director of Administration.
  - b. The Director of Administration must immediately inform Council and begin an investigation.
  - c. If the Council must respond to the complainant within five (5) business days following the receipt of the complaint. Council must outline the steps they will take to ensure a resolution and must report back to the party of the complaint within thirty (30) business days with their decision.

- d. During the thirty (30) business days, the Director of Administration will review all of the information, conduct interviews, consult legal counsel where required to ensure thoroughness and fairness.
- e. The Director of Administration will keep Council informed of the progress of the investigation at all times.
- f. A meeting will be called by the Director of Administration and the Council to review the information collected during the investigation.
- g. Council will deliver their decision in writing to the party to the complaint.
  - i. If a breach did occur, legal counsel will be sought on possible remediation measures and a report will be developed for the complainant.
  - ii. Council will work to ensure the breach in question is preventing in the future.
  - iii. If a breach did not occur, a report will be made to the complainant.

#### **F. References and Related Authorities**

None

#### **G. Appendices**

(1) Appendix F – Glooscap First Nation Breach of Privacy Complaints Form