Mnaasged Child and Family Services

Part X

Policy and Procedure Manual

March 2020

Acknowledging the Past
Serving the Present
Creating the Future

TABLE OF CONTENTS

SECTION 1: INTRODUCTION 1

Preamble 1

SECTION 2: CONSENT 3

Consent 3

SECTION 3: PRIVACY 11

Privacy 11

Privacy Breaches 13

Access and Corrections to Records 20

SECTION 1: INTRODUCTION

PREAMBLE

Part X of the *Child, Youth and Family Services Act* (CYFSA) is the section of the legislation that governs the collection, control, and usage of information by Service Providers. Part X came into force January 1, 2020.

As an Agency funded under the *Child, Youth and Family Services Act*, Mnaasged Child and Family Services is considered a Service Provider under Part X and is, therefore, required to follow the Standards concerning privacy and access to personal information gathered in the delivery of services to Children/Youth and families within its provincially funded Child Welfare Services. Mnaasged Child and Family Services has chosen to apply the same requirements across all services to ensure consistency.

The Office of the Information and Privacy Commissioner of Ontario has the authority under the *Child, Youth and Family Services Act* to oversee Part X.

Information collected, recorded, and used by Mnaasged Child and Family Services about a Parent, Child/Youth, other family member, or any other person identified in its records will be considered personal information. Mnaasged will be required to ensure the following when collecting personal information:

a) Have the consent of the person for whom the collected information concerns

b) Have consent for the usage and sharing of the information

c) Take steps to ensure the protection and safety of the information to prevent unauthorized disclosure or usage

d) Advise the person should there be any unauthorized disclosure or breach of the security to protect the information

e) Provide access to the person's record upon request

f) Take steps to correct any reported inaccuracies or gaps in information subsequently noted by the person

Exceptions to the above include the following:

1. If collected information is subject to federal legislation that prohibits or limits its disclosure (such as the *Youth Criminal Justice Act* or the *Criminal Code of Canada*), this legislation will supersede Part X.

2. If a Child/Youth has been adopted, the section of the *Child, Youth and Family Services Act* addressing disclosure of adoption-related information prevails over Part X.

SECTION 2: CONSENT

Department: All	POLICY #:
Section: Consent	
Subject: Consent	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act,* Part X	

CONSENT

POLICY

Consent is a key principle of privacy. Mnaasged Child and Family Services respects the rights of individuals to control their own personal information, subject to certain limits that are permitted or required by law. There are many situations where Mnaasged Child and Family Services requires consent to collect, use, or disclose information; however, no consent will be needed when it is required by law to protect the safety and well-being of Children/Youth.

Given that most Indigenous Societies use stories to gather, use, and transmit information from one generation to the next, Mnaasged Child and Family Services must exercise caution when collecting information from Indigenous communities that are transmitted through oral history or stories. Mnaasged Child and Family Services Employees must always seek consent before documenting this information.

If Mnaasged Child and Family Services is required to have an individual's consent to collect, use, or disclose personal information then this individual may choose to give full consent, may limit what can be done with the information, may choose to withhold consent, or may choose to withdraw consent once given on a go-forward basis.

PROCEDURE

ELEMENTS OF CONSENT

1. Consent will acknowledge the following:

a) Provided by the individual or a Substitute Decision Maker if the individual is incapable of making one's own decision

b) Not be obtained through deception or coercion

c) Relate to the information that is being collected, used, or disclosed

d) Be knowledgeable and informed

2. A consent will be considered knowledgeable if it is reasonable for Mnaasged to believe that the individual knows the following:

   a) Purpose of the collection, use, or disclosure of personal information

   b) Personal right to give, withhold, limit, or withdraw one's consent

3. Mnaasged will provide services to Children/Youth and families and will be required to inform them about their rights to privacy and the purposes for the collection of personal information so that they will understand and can make informed decisions about their own personal information.

4. Mnaasged will also be required to post its information practices and the purposes for which it collects, uses, and discloses personal information in places where it will be obvious to people receiving Mnaasged's services, such as the following:

   a) Mnaasged's website

   b) Mnaasged's communications material given to Children/Youth, families, and the public

   c) On the walls at Mnaasged locations where Children/Youth, families, and the public visit

CAPACITY

1. Everyone is presumed to be capable of making their own privacy decisions unless the presumption is unreasonable. For example, babies are never capable of making their own decisions. Very young Children are rarely able to make their own decisions about their personal information; however, as Children age, they may become more capable.

2. If an individual's capacity is questionable, capacity will be assessed on a case-by-case basis. Capacity to make information and privacy decisions will be a two-part test. When considering someone capable, a Child, Youth, or Adult must have the ability to comprehend the following:

   a) Understand the information that is relevant to one's decision to collect, use, or disclose that information

b) Appreciate the reasonably foreseeable consequences of one's choices about the collection, use, or disclosure of that information (give, not give, limit, or withdraw their consent)

3. If an individual is not able to understand the relevant information or appreciate the reasonably foreseeable consequences of personal information choices, it will be considered that the individual is incapable of making decisions on that information.

WHO CAN CONSENT

1. When consent is required under Part X of the *Child, Youth and Family Services Act* and Mnaasged's privacy policies, the following authorized persons may give consent:

   a) A capable individual older than 16 years of age

   b) A capable individual aged 16 years and older who authorizes in writing for another individual to be the Substitute Decision Maker

   c) For a Child/Youth younger than 16 years of age, the Parent or Guardian who has lawful custody

2. The Parent or Guardian with lawful custody may not consent if the information to be disclosed relates to "treatment" (as defined by the *Health Care Consent Act*, 1996) about which the Child/Youth has made their own decision.

3. The Parent or Guardian with lawful custody may not consent if the information to be disclosed relates to "counselling" (as defined by the *Child, Youth and Family Services Act*) about which the Child/Youth participated on their own. Therefore, if a Child/Youth provided consent to treatment or counselling, a Parent or Guardian cannot consent to the release of that information on behalf of the Child/Youth.

4. If a disagreement occurs between a capable Child/Youth and the Parent or Guardian with lawful custody about the release of personal information, the capable Child's/Youth's wishes will prevail.

5. If Helpers have questions about consent for Children/Youth, the issue will be discussed with their Supervisor (who may suggest consultation with Mnaasged's Privacy Lead or Legal Counsel.

6. The following is a prioritized list of possible Substitute Decision Makers:

   a) Substitute Decision Maker under the *Health Care Consent Act* for specific purposes (identity must be verified by checking identification and other documentation)

b) Guardian of the person or Guardian of the property if the consent relates to the Guardian's authority to make decisions on behalf of the individual (copy of the related documentation must be seen)

c) Individual's Attorney for personal care or Attorney for property if the consent relates to the Attorney's authority to make decisions on behalf of the individual (copy of the related documentation must be seen)

d) Individual's Representative appointed by the Consent and Capacity Board if the Representative has the authority to give consent (copy of the related documentation must be seen)

e) Individual's spouse or partner

f) Child/Youth, Parent, Children's Aid Society, or other person who is lawfully entitled to give or refuse consent in the place of the Parent (this does not include a Parent who has only a right of access to the individual)

g) Parent of the individual with only a right of access to the individual

h) Sibling of the individual

i) Any other relative of the individual

j) Estate Trustee in the case of a deceased individual (unless the individual has been deceased for more than 30 years, in which case the information is no longer personal information)

7. If a person outranks another person lower on the above list, the higher ranked person will be the Substitute Decision Maker.

8. The identity of the Estate Trustee will be verified by reviewing a will or the notarized "Certificate of Appointment of Estate Trustee with a Will" or "Certificate of Appointment of Estate Trustee without a Will." A copy of this documentation must be uploaded and kept in the Child Protection Information Network.

9. If a deceased individual does not have an Estate Trustee, consent can be obtained from the person who assumed responsibility for the administration of the deceased individual's estate if documented in writing.

10. If Staff have questions regarding Substitute Decision Makers, the issue will be discussed with their Supervisor (who may suggest consultation with Mnaasged's Privacy Lead or Legal Counsel).

NO CONSENT

1. There are certain circumstances for which Mnaasged does not need consent to collect, use, or disclose personal information because these activities are permitted or required by law, such as in the following situations:

    a) Anyone if they reasonably suspect that a Child/Youth may need protection are required to report to a Child Well-Being Agency or to a Children's Aid Society. Part X privacy obligations are not a barrier to the collection or disclosure of information reasonably necessary to assess, reduce, or eliminate the risk of harm to a Child/Youth

    b) Share personal information with other Child Well-Being Agencies, Children's Aid Societies (includes searches of the Child Protection Information Network and Fast Track), or Child Welfare authorities outside Ontario if the information is reasonably necessary to assess, reduce, or eliminate a risk of harm to a Child/Youth

    c) Use or disclose personal information if there is a belief on reasonable grounds that it is reasonably necessary to assess, reduce, or eliminate a risk of serious harm to a person or group

    d) Consult or plan with a representative chosen by each of the Child's/Youth's First Nation, Métis, or Inuit community

    e) Collect information from an incapable person if the collection is reasonably necessary for the following:

        i. Provide a service if it is not possible to obtain consent (for example, from a Substitute Decision Maker) in a timely manner

        ii. Assess, reduce, or eliminate a risk of serious harm to any person or group

        iii. Assess, reduce, or eliminate a risk of serious harm to a Child/Youth

    f) Disclose personal information when reasonably necessary to a Law Enforcement Agency in Canada to aid in an investigation

    g) Disclose personal information to the Ministry of Children, Community and Social Services if asked to do so in accordance with its powers

    h) Engage in risk and error management, quality improvement, or assurance activities

    i) Contact a relative, friend, or potential Substitute Decision Maker in certain instances, such as when an individual is injured or incapacitated

    j) Dispose of or de-identify the information

k) Engage in some research projects (subject to certain rules, such as obtaining research ethics boards' approvals of research plan)

l) Respond to legal proceedings if Mnaasged is or expected to be a party or witness and the information relates to a matter at issue

2. Part X of the *Child, Youth and Family Services Act* permits the non-consensual disclosure of information if reasonably necessary to fulfill an Agency's statutorily mandated functions. What is reasonably necessary may differ between Indigenous and non-Indigenous Children/Youth. For instance, given the heightened role played by extended family members in the lives of some Indigenous Children/Youth, it may be necessary to share information with a broader circle of people when providing Indigenous culturally appropriate services.

3. Circle processes for dispute resolution require the complete disclosure and the complete confidentiality of relevant information. These requirements should inform what is considered "reasonably necessary" disclosure.

4. If Helpers have questions regarding collecting, using, or disclosing personal information without consent, the issue will be discussed with their Supervisor (who may suggest consultation with Mnaasged's Privacy Lead or Legal Counsel).

CONSULTATION REQUIREMENTS UNDER THE *CHILD, YOUTH AND FAMILY SERVICES ACT*

1. The *Child, Youth and Family Services Act* requires Agencies to consult with Indigenous communities. Mnaasged will share sufficient information with an Indigenous community's Representative to enable meaningful consultation and engagement. These obligations are set out in sections 72 and 73 of the Act. The obligation to consult with Indigenous communities is not impacted by Part X.

EXPLICIT CONSENT

1. Other than as permitted or required by law, Mnaasged will seek explicit consent from an individual (or the Substitute Decision Maker) to achieve the following:

a) Directly collect personal information from an individual (or the Substitute Decision Maker) for a purpose other than to provide a service

b) Indirectly collect personal information (i.e., from a third-party source)

c) Use personal information to provide a service if the personal information was collected indirectly or use it for a purpose other than providing a service

d) Disclose personal information

2. Explicit consent can be given in writing or orally. If given orally, Mnaasged will document the consent in a Contact Log in the Mnaasged Information Management System as well as include the following information:

    a) Name of the individual who gave the consent

    b) Personal information to which the consent relates

    c) Details about informing the individual on the purposes of the collection, use, or disclosure of the personal information

    d) Details about informing the individual of the right to place limits on the consent and to withdraw the consent at any time

3. The written explicit consent will be documented on the Consent to Collect, Use, or Disclose Personal Information Form (Appendix 1). The form will be completed in full by the individual or the Substitute Decision Maker. If there are any accessibility issues, a Helper will assist in completing this form as the individual wishes. This will be documented in the Contact Log.

4. If seeking Personal Health Information of an individual, the Helper may choose to obtain consent from the individual or the Substitute Decision Maker documented on the Consent to Disclose Personal Health Information Form (Appendix 2). Many health information custodians will require this completed form to obtain medical or mental health assessments or reports.

IMPLIED CONSENT

1. A Helper can rely on implied consent when collecting information directly from an individual or the Substitute Decision Maker for the purpose of providing the individual with a service. Therefore, it will not be a requirement to seek permission to collect or use this information. When personal information is directly collected from a Client, the Helper will still be required to explain what will be done with the information.

2. A Client's request for service constitutes implied consent to use personal information for the purpose of providing service unless the Client explicitly instructs otherwise.

CONDITIONAL CONSENT

1. When A Helper needs an individual's consent to collect, use, or disclose personal information, the individual may add limits or place conditions on that consent. The individual may choose to share parts of the personal information with certain people but not others.

2. If an individual requests a restriction or places limits on the use of the personal information, the Helper will comply with those instructions unless the following occurs:

a) Information is reasonably necessary to assess, reduce, or eliminate a risk of serious harm to any person or group

b) Information is reasonably necessary to assess, reduce, or eliminate a risk of harm to a Child/Youth

POLICY REFERENCE

SECTION 3: PRIVACY

Department: All	POLICY #:
Section: Privacy	
Subject: Privacy	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Part X	

PRIVACY

POLICY

Mnaasged Child and Family Services strives to create and maintain working relationships that are built on a foundation of trust and privacy. Mnaasged Child and Family Services recognizes the privilege it holds in collecting, using, and retaining records related to the most vulnerable and sensitive moments of its Clients' lives and, therefore, is committed to treating this information with the utmost care and respect.

As an Indigenous Child Well-Being Agency, Mnaasged Child and Family Services recognizes that the Child, Youth and Family Services Act*, including the privacy provisions, requires Service Providers to deliver all services to Indigenous Children/Youth, families, and communities in a manner that "recognizes their individual traditions, heritage, and connections to their Indigenous communities." Mnaasged Child and Family Services also recognizes that not all Indigenous communities have the same practices and underlying values with respect to the gathering, use, and dissemination of information. Mnaasged Child and Family Services understands that Indigenous families are overrepresented in Ontario's Child Welfare System and, as such, are disproportionately affected by the misuse, loss, and denial of access to personal information.*

Mnaasged Child and Family Services acknowledges that the information it holds belongs to the individual, and Mnaasged Child and Family Services respects an individual's right to make decisions regarding one's own information and privacy. Mnaasged Child and Family Services believes that Clients should be empowered to have control of their information and their story, which includes their right to access their records and request corrections to information that has been recorded incorrectly or incompletely. Employees of Mnaasged Child and Family Services have an obligation to record information in a strengths-based, anti-oppressive manner. Mnaasged Child and Family

Services recognizes that Clients have the right to formally complain through the Information Privacy Commissioner of Ontario if they feel their privacy has been compromised, find that their information was recorded incorrectly or seen through an oppressive or prejudicial lens, or find that their information was not captured in a fulsome way. Mnaasged Child and Family Services recognizes privacy as a human right of its Clients, Foster Parents, Volunteers, and Staff and is committed to fostering a culture of privacy within its Agency that is reflective of this human right.

PROCEDURE

POLICY REFERENCE

Department: All	POLICY #:
Section: Privacy	
Subject: Privacy Breaches	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act,* Part X	

PRIVACY BREACHES

POLICY

Mnaasged Child and Family Services will ensure that all Privacy Breaches concerning information collected and stored with and in the possession of or otherwise accessed by Staff, Volunteers, Alternative Care Providers, or Board Members concerning identifiable persons will be addressed in a manner that is consistent with this Policy and Procedure and in keeping with the legislated requirements of Part X of the Child, Youth and Family Services Act *(CYFSA).*

PROCEDURE

1. Mnaasged requires all Staff, Alternative Caregivers, Contractors, Volunteers, and Students (collectively referred as "Team Members") to report all privacy complaints, incidents, and actual or potential breaches immediately to the immediate Supervisor and Mnaasged's Privacy Designate (Director of Services or designate).

2. Types of privacy complaints, incidents, or breaches include but are not limited to the following examples:

    a) Mnaasged's server is hacked and held ransom after an email with a virus is opened

    b) Unencrypted laptop with personal information saved on the hard drive is stolen

    c) Courier package of a Client's records is not delivered to the correct address

    d) Unencrypted USB key with an Excel spreadsheet or word files with Client information is lost

    e) Team Member talks about a case with a friend and discloses personal information about the Children/Youth involved

f) Team Member takes a picture or makes an audio or video recording of a Client without the knowledge or consent of the Client

g) Team Member sends an email to a "Help Desk" attaching a worksheet with Client information but does not check the email address and, instead of sending the attachment internally, sends it to the last Help Desk emailed, which is at a bank

h) Paper records of case files to be disposed are recycled and not shredded

i) Out of curiosity, a Team Member reviews a neighbour's electronic personal record

j) Student looks at Client information in the Mnaasged Information Management System on a self-initiated education project without being assigned to those cases or people

k) Fax with personal information is misdirected to a business because the fax number was entered incorrectly

l) Team Member writes a post on social media about a case with enough detail that the Child/Youth and family would be identifiable to certain people

3. The following steps will be taken by the Privacy Designate if it is believed there has been a privacy breach:

STEP 1: RESPOND IMMEDIATELY BY IMPLEMENTING THE PRIVACY BREACH PROTOCOL

1. Ensure that the appropriate individuals are immediately notified of the breach, including the appropriate Helper, Supervisor, and Senior Manager whose Clients are potentially affected by the privacy breach.

2. Inform the Director of Service (if not acting as Privacy Designate) who will advise on addressing the priorities of containment and notification as set out in the following steps:

   a) Consider if notification to the Information and Privacy Commissioner of Ontario (IPC/O) (www.ipc.on.ca) will be required and, if not, will be advisable (see section on Mandatory Notification below). The Privacy Designate must revisit this need to report on an ongoing basis as it may be premature to report if unclear there has been a breach or of the scope of the breach. The Privacy Designate may need to keep the Information and Privacy Commissioner of Ontario apprised throughout this process

   b) Consider if notification to the Ministry of Children, Community and Social Services will be required and who would do so on behalf of Mnaasged

   c) Consider when to notify the insurer (which may be a condition of coverage), the Executive Director, the Executive Committee, the Board Chair, and other key internal stakeholders

d) Consider alerting the Communications Department

e) Consider notifying the Police

STEP 2: CONTAINMENT – IDENTIFY THE SCOPE OF THE POTENTIAL BREACH AND TAKE STEPS TO CONTAIN IT

1. Retrieve and secure any personal information that has been disclosed or inappropriately used or collected (including all electronic and hard copies). This might include attending at the scene to determine whether there are any other records out in public.

2. Ensure that no copies of personal information have been made or retained by the individual who was not authorized to collect or use the information. Obtain the person's contact information if follow-up will be required.

3. Determine whether the privacy breach would allow unauthorized access to any other personal information (e.g., Mnaasged Information Management System) and take whatever necessary steps are appropriate (e.g., change passwords or identification numbers, temporarily shut down a system, suspend an individual's or group's access to the system, implement security, and institute a restriction to the file).

STEP 3: CLARIFY THE FACTS

1. Consider if there is sufficient expertise to conduct an Internal Investigation and if a specialist (such as a privacy or Information Technology security specialist) will be required.

2. Determine how it happened, who was involved, why, and the scope of the breach by answering the following:

    a) Details of the incident and how it was discovered

    b) Number of people affected

    c) Who was involved

    d) Dates

    e) Type of incident, such as the following:

        i. Unauthorized use

        ii. Unauthorized disclosure

        iii. Hacking, malware, or security breach

        iv. Lost or stolen mobile device

v. Lost or stolen hard copies

vi. Fax to wrong number

vii. Email to wrong recipient

STEP 4: NOTIFICATION – IDENTIFY THOSE INDIVIDUALS WHOSE PRIVACY WAS BREACHED AND NOTIFY THEM OF THE BREACH

1. At the first reasonable opportunity, any affected individuals whose privacy was breached will be notified. Careful consideration will go into whether there is a need to inform affected individuals immediately (especially if the breach is ongoing, the information in question is of a highly sensitive nature, or there is reason to believe that it will be used in a malicious way).

2. The type of notification will be determined based on the circumstances, such as the sensitivity of the personal information, the number of people affected, and the potential effect the notification will have on the individual(s). Some examples of notification include the following:

   a) In person, by telephone, in writing, or a notation made in the file to be discussed at the next meeting, depending on the circumstances

   b) Public notice as the most efficient and effective method of notice

3. When providing notification, Mnaasged will focus on the following considerations:

   a) Potential privacy impact of calling the individual's home or sending a letter

   b) Whether the affected individual will be seeing a Helper very soon and could be told in person

   c) Whether anyone affected is in a vulnerable state of health, deceased, or incapable to make decisions such that notice would be given to a Substitute Decision Maker and consider what is the best way to manage those sensitive issues

   d) Details of the extent of the breach and the specifics of the personal information at issue

   e) Steps that have been or will be taken to address the breach, both immediate and long-term, to ensure the following:

      i. Reduce potentially harmful effects on the individual

      ii. Prevent a similar breach from happening

   f) Contact information for a Team Member who can provide additional information to the affected individuals

g) Affected individuals have the right to complain to the Information and Privacy Commissioner of Ontario

h) Establish a plan to address what Staff and others should do if they receive calls about the privacy breach

i) Consider notifying the Information and Privacy Commissioner of Ontario and the Ministry, especially if required by law to do so (see Mandatory Notification below), or Legal Counsel if appropriate

STEP 5: INVESTIGATION AND REMEDIATION

1. Conduct an Internal Investigation into the matter. The objectives of the investigation will consider the following:

   a) Ensure the immediate requirements of containment and notification have been addressed

   b) Review the circumstances surrounding the breach

   c) Review the adequacy of existing policies and procedures in protecting personal information

   d) Address the situation on a systemic basis

   e) Identify opportunities to prevent a similar breach from happening in the future

   f) Change practices as necessary

2. Ensure that Team Members are appropriately re-educated and retrained with respect to the compliance with the privacy protection provisions of the *Child, Youth and Family Services Act*, 2017, the circumstances of the breach, and the recommendations of how to avoid it in the future.

3. Continue notification obligations to affected individuals as appropriate.

4. Consider notifying the Information and Privacy Commissioner of Ontario or Legal Counsel as appropriate.

5. Consider any disciplinary consequences with Staff or any contract issues with independent Contractors or Vendors that follow from the privacy breach and any related obligations to report to regulatory colleges.

STEP 6: RECORDKEEPING

1. Staff will keep a record of all privacy complaints, incidents, and breaches including investigations, notifications, and remedial actions taken.

2. Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information will be submitted to the Information and Privacy Commissioner of Ontario annually, which is due each March for the previous calendar year. The Information and Privacy Commissioner of Ontario will provide an electronic form and guidance for submitting the statistical report on its website.

MANDATORY NOTIFICATION

1. Mnaasged will abide by its obligations to notify or report to the Information and Privacy Commissioner of Ontario and the Ministry of Children, Community and Social Services as required by law. Mnaasged will take guidance from the Information and Privacy Commissioner of Ontario based on its interpretation of the reporting obligations found at https://www.ipc.on.ca/part-x-cyfsa/safeguarding-and-managing-personal-information/responding-to-privacy-breaches/

2. Privacy breaches that meet the following criteria must be reported to the Information and Privacy Commissioner of Ontario and the Ministry of Children, Community and Social Services:

    a) Mnaasged has reasonable grounds to believe that the personal information was used or disclosed without authority by a person who knew or ought to have known that the person was using or disclosing the information without authority

    b) Mnaasged has reasonable grounds to believe that the personal information was stolen

    c) Mnaasged has reasonable grounds to believe that the personal information that was stolen or lost or used or disclosed without authority was or will be further used or disclosed without authority

    d) The loss or unauthorized use or disclosure of the personal information is part of a pattern of similar losses or unauthorized uses or disclosures of personal information in Mnaasged's custody or control

    e) Mnaasged has reasonable grounds to believe that personal information that Mnaasged disclosed to an approved entity (such as the Institute of Clinical Evaluative Sciences or the Canadian Institute for Health Information) or a non-approved person or entity under sections 293(1), (2), or (3) of the *Child, Youth and Family Services Act*, 2017, has been stolen or lost or used or disclosed without authority by the approved entity or the non-approved person or entity

    f) Team Member is terminated, suspended, or disciplined as a result of the theft, loss, or unauthorized use or disclosure of personal information by the Team Member

    g) Team Member resigns and Mnaasged has reasonable grounds to believe that the resignation is related to an investigation or other action by Mnaasged with respect to

the theft, loss, or unauthorized use or disclosure of personal information by the Team Member

h) Mnaasged determines that the loss or unauthorized use or disclosure of the personal information is significant after considering all relevant circumstances, including the following:

   i. Sensitivity of the personal information that was lost, used, or disclosed without authority

   ii. Volume of the personal information that was lost, used, or disclosed without authority

   iii. Number of persons whose personal information was lost, used, or disclosed without authority

   iv. If one or more Service Providers were involved in the loss or unauthorized use or disclosure of the personal information

POLICY REFERENCE

Department: All	POLICY #:
Section: Access and Corrections to Records	
Subject: Access and Corrections to Records	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Part X	

ACCESS AND CORRECTIONS TO RECORDS

POLICY

All individuals regardless of age have a right to access their personal records in the custody or control of Mnaasged Child and Family Services that relate to their service provision. Part X will apply to the general right of access to all records of personal information in the custody or control of Mnaasged Child and Family Services, regardless of where the information originated. The right of access will not be limited to records in the custody or control of a Service Provider that were created by Mnaasged Child and Family Services.

PROCEDURE

The following procedural steps were taken from Part X of the *Child, Youth and Family Services Act* section on "A Guide to Access and Privacy for Service Providers" produced by the Information and Privacy Commissioner of Ontario that has jurisdiction for monitoring and managing issues related to the administration of Part X.

1. There are a few exceptions to the right of access. On receiving a request for access to personal records or a disclosure of a portion of the records, the Helper responsible will review the record to determine if any of the following apply:

    a) Individuals do not have a right to access their record of personal information if the following apply:

        i. It is subject to a legal privilege restricting its disclosure to the individual

        ii. Another Act or a Court Order prohibits its disclosure to the individual

        iii. Information was collected or created primarily in anticipation of a legal proceeding that has not been concluded

b) Individuals do not have a right to access their record of personal information if granting access could reasonably be expected to result in the following:

i. Risk of serious harm to any individual

ii. Identification of an individual in the record who was required by law to provide information to Mnaasged

iii. Identification of an individual who provided the information either explicitly or implicitly in confidence and Mnaasged considers it appropriate to keep the identity confidential

2. If one of these exceptions applies, the individual does not have a right to access that information in the record. However, the Helper would still be required to grant access to the remainder of the record if the Helper can sever or redact the information to which the exception applies.

3. Before disclosing, the Helper and the Supervisor will ensure the removal of any information that falls within these exceptions. Where there is any uncertainty, a consultation or review by Legal Counsel or the Director of Services or designate will occur.

4. In addition to these exceptions, Part X will allow Mnaasged to refuse access if a request is "frivolous or vexatious" or made in bad faith. A request is frivolous or vexatious if it is part of a pattern of conduct (such as an excessive number of access requests by the same person) that amounts to an abuse of the right of access, interferes with the operations of Mnaasged, or is made for a purpose other than to obtain access (such as to annoy or to harass Mnaasged or to purposefully burden the system). There is a high threshold for deciding a request is considered frivolous or vexatious. Refusing an access or a request for a correction on these grounds will not be a routine matter and will not be taken lightly.

5. If it is believed that a request is vexatious, Legal Counsel will be consulted.

6. If the record is dedicated primarily to the provision of service to the individual requesting access, the individual will be entitled to access or disclosure of the entire record (subject to the exceptions previously noted) even if it incidentally contains information about other individuals or other matters.

7. If the record is not dedicated primarily to the provision of service to the individual requesting access, the individual only has a right to their own personal information that can reasonably be severed from the rest of the record. For example, a Youth who was in Care wishing to access personal records that contain incidental information about other persons such as Foster Parents of family members will still be entitled to the record pertaining to the Youth.

8. Establishing whether a record is dedicated primarily to providing services to the individual will be important because it determines what access the individual will have to a record.

The provision of a service to the individual will be central to the purpose for which the record exists if any of the following occur:

a) Record only exists because of the provision of service to the individual

b) Record is not qualitatively related to other matters, such as legal advice

c) Record would typically be found in an individual's file

9. It may not always be the case that every record filed under an individual's name will be dedicated primarily to providing services to that person. Determining whether a record is dedicated primarily to the provision of service to the person requesting access will be done on a record-by-record basis.

10. Records will be reviewed to ensure that they are directly related to the individual seeking access or disclosure.

HOW ARE ACCESS REQUESTS MADE?

1. Mnaasged may choose to respond to verbal or informal requests for access, but a request must be in writing for the procedural access rules of Part X to apply. There is no requirement in the *Child, Youth and Family Services Act* for individuals to use a certain form or to submit the request in a certain way. Whether there is a preference for individuals to make access requests by filling out a designated form, Mnaasged must still respond to requests that come in other formats, such as email.

2. There is no requirement for a person requesting access to a record to specify that they are seeking access under Part X of the *Child, Youth and Family Services Act*. However, it may be helpful to clarify this with the individual requesting access in certain circumstances, such as where more than one privacy and access law could apply.

3. Access requests must include enough detail to enable the Helper to identify and locate the record with reasonable effort; for example, if the Helper determines on reviewing the information that there are several people who have the same name, further information will be needed to verify that the information relates to the same individual requesting access. If a request does not contain enough detail, the Helper will offer assistance to the individual requesting access in clarifying the request. This should be done on receipt of a request that is not sufficiently detailed. Once the request contains sufficient detail, a 30-day timeline for a response will begin.

MNAASGED'S RESPONSE TO ACCESS REQUESTS

1. When Mnaasged receives an information access request, a Helper will conduct a reasonable search to locate the record(s). A reasonable search means an experienced Employee made a reasonable effort to locate the records.

2. Mnaasged must respond to an access request as soon as possible and no later than 30 calendar days after receiving the request. If Mnaasged does not respond within 30 days, this will be deemed as refusing the request. The individual may then make a complaint to the Information and Privacy Commissioner of Ontario.

3. In some cases, an individual may request expedited access; for example, an individual may explain the information is needed within two (2) weeks to meet an application deadline for a specific program or service. If the Helper is satisfied with the evidence that access is required in an expedited period, the Helper will grant access within that period if reasonably able to do so.

4. Outside of expedited access requests, the Helper's response will be due within 30 calendar days. The response will provide one or more of the following:

    a) Grant access to some of or all the requested information

    b) Refuse or decline access to some of or all the information with a written explanation

    c) Extend the deadline to fully respond within 90 days with a written explanation

5. These responses will not be mutually exclusive; for example, a response might grant access to some information while refusing access to other information.

GRANTING ACCESS

1. Granting access means giving the person requesting it the opportunity to examine a record and, at their request, to receive a copy of the record. It is not sufficient to provide a summary of the record. If it is practical to do so, the Helper will explain the purpose and the nature of the record and any terms, codes, or abbreviations used.

2. A fee cannot be charged for providing access to a record. This rule applies to all activities associated with processing an access request; for example, there cannot be a charge for filing the request, photocopying, postage, or Staff time required to process the request.

3. Before providing access, a Helper must take reasonable steps to ensure the identity of the individual requesting access. In some cases, this might include the individual signing a confirmation form or showing official identification.

REFUSING OR DECLINING ACCESS

1. The written response may also indicate that no access will be provided to some of or all the requested records. If a Helper cannot locate a record after a reasonable search or has concluded that the record does not exist, cannot be found, or Part X does not apply then this will be clearly indicated in the response to the individual requesting access. The Helper will inform the individual requesting access of the right to file a complaint to the Information and Privacy Commissioner of Ontario.

2. If the Helper refuses all or part of the request based on one of the access exceptions, the Helper will give written notice to the individual requesting access of the refusal and the entitlement to complain to the Information and Privacy Commissioner of Ontario. In most cases the Helper will be required to inform the individual requesting access of any exceptions that may apply, such as the following:

    a) Information is subject to a legal privilege

    b) Another Act or a Court Order prohibits disclosure to the individual

    c) Request is frivolous or vexatious or made in bad faith

3. Helpers will have discretion about how to inform the individual requesting access when one of the access exceptions apply. The Helper can choose to specifically indicate the exception that applies or that one of them applies without specifying which one. The Helper can also refuse to confirm or deny the existence of any record subject to the following exceptions:

    a) Information was collected or created primarily in anticipation of a legal proceeding that has not been concluded

    b) Granting access could reasonably be expected to result in a risk of serious harm to any individual

    c) Identification of an individual in the record who was required by law to provide information to Mnaasged

    d) Identification of an individual who provided the information either explicitly or implicitly in confidence and it is considered appropriate to keep the identity confidential

EXTENDING THE DEADLINE

1. In limited circumstances, Mnaasged may advise an individual that a deadline will be extended for responding to a request for access by not more than 90 calendar days. An extension will be allowed in the following circumstances:

    a) Response within 30 days would unreasonably interfere with Mnaasged operations because the request involves numerous pieces of information or requires a lengthy search

    b) Assessment of the individual's right of access is not feasible within the 30 days

2. If a Helper plans to extend the deadline, a written notice of the length of the extension and the reason for it will be given to the individual no later than 30 days after receiving the original request. The Helper must then provide a full response, granting or refusing access, within the extended time limit. Otherwise, the Helper will be deemed to have refused the request. Individuals will be entitled to file a complaint with the Information and Privacy

Commissioner of Ontario for any refusal of a request for access, including a deemed refusal. They can also complain about the time extension itself; for example, if individuals do not agree that their request for access meets the criteria for an extension under Part X.

SUBSTITUTE DECISION MAKERS CAN REQUEST ACCESS

1. A Substitute Decision Maker can request access to personal records on an individual's behalf; for example, the Parent or Guardian of a Child/Youth younger than 16 years old who is receiving services from Mnaasged may request access to the Child's/Youth's records. This would be an access request under sections 312 to 314 of the *Child, Youth and Family Services Act*, rather than a disclosure. Any reference to the individual in Part X would be read as a reference to the Substitute Decision Maker; for example, the requirement to respond to the individual within 30 days would be read as a requirement to respond to the Substitute Decision Maker within that time frame.

2. A Substitute Decision Maker has the authority to request access unless it is unreasonable to do so. However, it is an offence under the *Child, Youth and Family Services Act* to make an access or correction request under false pretenses.

3. When a Substitute Decision Maker requests access on behalf of a capable Child/Youth, the decision of the capable Child/Youth will prevail if there is a conflict. For example, a Parent or Guardian requests access to their 14-year-old Youth's records, but the Youth indicates that no access should be granted to the Parent or Guardian. Provided the Youth is capable, this decision will prevail, and the Parent's or Guardian's request for access will be refused.

INDIVIDUAL'S RIGHT TO CORRECTION OF RECORDS

1. Under Part X, individuals have the right to request a correction to records of their personal information, with limited exceptions. As with access requests, Mnaasged will respond to requests for correction within 30 calendar days and will not be permitted to charge fees. In the following section, individuals' correction rights, exceptions, and detailed rules for how to respond will be reviewed.

2. Individuals may request that Mnaasged correct a record of their personal information if they believe it is inaccurate or incomplete. A Substitute Decision Maker may also request a record correction on behalf of an individual. A correction refers not only to striking out incorrect information but also to adding information.

3. There is no age requirement for making a request for a correction. The right to request a correction from Mnaasged only applies if Mnaasged has previously given the individual access to the record.

4. Individuals must submit requests for a correction to Mnaasged in writing. The law does not require the use of a certain form nor submit the written request in a certain manner. This means that even if Mnaasged prefers for individuals to make correction requests using a

designated form, Mnaasged must still respond to requests that come in other formats, such as through email.

5. Mnaasged must grant a request for a correction if the individual satisfactorily demonstrates that the record is inaccurate or incomplete and provides the information needed to correct the record.

6. Mnaasged is not required to correct a record if the following occurs:

    a) Information consists of a professional opinion or observation that was made in good faith

    b) Mnaasged did not create the information and does not have sufficient knowledge, expertise, or authority to correct it

    c) Reasonable grounds to believe the request is frivolous or vexatious or made in bad faith

MNAASGED'S RESPONSE TO CORRECTION OF RECORDS REQUESTS

1. The timelines and other rules for responding to a request for correction are very similar to those for requests for access. Mnaasged must respond to a correction request as soon as possible and no later than 30 calendar days after receiving the request. If Mnaasged does not respond within 30 days, it will be deemed as refusing the request, and the individual may then make a complaint to the Information and Privacy Commissioner of Ontario.

2. Mnaasged's response within 30 days will be in writing and will explain the actions of one or more of the following:

    a) Granting the request for correction in whole or in part

    b) Refusing the request for correction in whole or in part, with a written explanation

    c) Extending the deadline to fully respond within 90 days, with a written explanation

GRANTING THE CORRECTION

1. When a request for correction is granted, a written notice of how the correction was made will be provided. Correcting means the following:

    a) Recording the correct information in the record or, if not possible, ensuring a system is in place to inform those who access the record that it is incorrect or incomplete and to direct them to the correct information

    b) Striking out the incorrect information without destroying it or, if not possible, by labelling it incorrect, severing it, storing it separately, and maintaining a link to trace back to the incorrect information

2. At the request of the individual, a written notice of the correction will be provided to the people to whom the information has been disclosed and to the extent it is reasonably possible. An exception to this requirement will be when providing a notice cannot reasonably be expected to affect the ongoing provision of services. Mnaasged will not charge a fee for granting a correction. This will apply to all activities associated with processing a request for a correction.

REFUSING THE CORRECTION REQUEST

1. A written response may indicate that some or all the requested corrections will not be made. In this case, an explanation of the refusal will be given, and the individual will be informed of the right to file a complaint with the Information and Privacy Commissioner of Ontario.

2. Additionally, the individual will be informed of the right to prepare a concise statement of disagreement regarding the correction that was refused and the right to require Mnaasged to ensure the following:

    a) Attach this statement to the record and disclose it whenever related information is disclosed

    b) Make reasonable efforts to provide the statement to any person who was previously disclosed of the information, unless the statement cannot be expected to affect the ongoing provision of services

EXTENDING THE DEADLINE

1. In limited circumstances, the deadline may be extended for responding to a request for a correction by no more than 90 calendar days**.** The deadline will be extended only if any of the following occur:

    a) Responding within 30 days would unreasonably interfere with Mnaasged operations

    b) It is not reasonably practical to respond within the 30 days, given the time required to complete the necessary consultations

2. If the deadline is extended, a written notice of the length of the extension and the reason for it must be provided to the individual within 30 days of receiving the request. A full response must be provided to grant or refuse the correction within the extended time limit. Otherwise, it will be deemed the request has been refused. For any refusal of a request for a correction, including a deemed refusal, an individual may file a complaint with the Information and Privacy Commissioner of Ontario. An individual may also complain about the time extension itself if the individual does not agree that the request meets the criteria where an extension is permitted under Part X.

POLICY REFERENCE