Mnaasged Child and Family Services

Information Services, Equipment, and Agency Records

Policy and Procedure Manual

July 2019

Acknowledging the Past
Serving the Present
Creating the Future

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

PREAMBLE

Mnaasged Child and Family Services (Mnaasged) recognizes the vital importance of Information Technology (IT) systems within the organization to support Employees in completing work functions and to assist in meeting Ministry standards regarding child welfare. Information Technology systems are to be used in a responsible, ethical, and legal manner consistent with the Mission and Values of Mnaasged as published throughout all Policy and Procedure Manuals.

The Information Technology Department will be responsible for maintaining a secure and stable Information Technology infrastructure, which includes, but is not limited to, workstations, computer software, servers, and access to networks such as the Mnaasged network or the internet.

The primary intent of this Manual is to encourage appropriate use and development of Mnaasged Information Technology-related resources and to outline how the Information Technology Department will accomplish this mission.

SECTION 2: INFORMATION TECHNOLOGY DEVELOPMENT

Department: Information Technology	POLICY #:
Section: Information Technology Development	
Subject: Decision-making and Impacting Information Technology Infrastructure	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

DECISION-MAKING AND IMPACTING INFORMATION TECHNOLOGY INFRASTRUCTURE

POLICY

Mnaasged Child and Family Services will ensure that any new infrastructure technology requirements for the organization will need the approval of Senior Management prior to implementation.

PROCEDURE

1. The Systems Administrator will research the impact on the Information Technology system in Mnaasged when required.
2. The Systems Administrator will research options and will make recommendations via a report to the Director of Finance and Administration.
3. The Director of Finance and Administration will review the report with Senior Management.
4. Upon approval of Senior Management, changes or upgrades to the system will follow regular purchasing policies as indicated in the Financial Policy and Procedure Manual.
5. The Director of Finance and Administration will direct the Systems Administrator to address the recommendations.
6. The Systems Administrator is responsible for informing all Mnaasged Staff by email notification about system upgrades.
7. When a report is not approved, the Director of Finance and Administration will notify the Systems Administrator. The Systems Administrator will explore other alternatives.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Information Technology Development	
Subject: Information Technology Systems	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

INFORMATION TECHNOLOGY SYSTEMS

POLICY

Mnaasged Child and Family Services will ensure that Information Technology systems are secure.

PROCEDURE

1. The Systems Administrator will be responsible for managing and maintaining the infrastructure of Mnaasged.
2. The Systems Administrator and other Staff of the Information Technology Department will ensure that systems are always operational.
3. The Systems Administrator will maintain a detailed diagram layout of the Mnaasged's network diagram.
4. The Network Technicians will ensure that all systems of Mnaasged have adequate security and are monitored and verified daily.
5. The Network Technicians will ensure that servers are monitored and backed up daily.
6. The Systems Administrator will develop and maintain an Information Technology guide to document all processes and procedures related to software and hardware operations used within the Information Technology Department.
7. The Systems Administrator will ensure that the Information Technology Infrastructure is reviewed regularly for improvements. Recommendations will be brought forward to the Director of Finance and Administration for review and approval by Senior Management.

8. When there are Information Technology-related issues and there is an absence of Staff in the Information Technology Department, the Director of Finance and Administration will be notified and consulted.

9. The Director of Finance and Administration will contact an approved Third-Party Provider to assist in resolving system issues until the Information Technology Department can resume normal functions.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Information Technology Development	
Subject: Information Technology Training	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

INFORMATION TECHNOLOGY TRAINING

POLICY

Mnaasged Child and Family Services will ensure that software training is provided to all Staff.

PROCEDURE

1. The Information Technology Department will develop an Information Technology training plan for all Mnaasged Staff. The training plan will include training activities for all system applications utilized by Mnaasged, such as Child Welfare Database, email, document creation, and access to other software application systems introduced to Mnaasged.

2. The Information Technology Department will develop and publish training documentation to be accessed by Staff through an internal intranet-based site. A Staff member from the Information Technology Department will be made available by special request to provide to staff further training on software packages on a one-to-one basis or in a classroom setting. The Systems Administrator must approve all additional training requests first.

3. If Information Technology Staff are unavailable or knowledge is limited for training Mnaasged Staff on software, the Systems Administrator and the Director of Finance and Administration will determine if a third-party firm is required.

4. Training will follow the guidelines set out in the Human Resources Policy and Procedure Manual: Training and Development Policy.

POLICY REFERENCE

Human Resource Policy and Procedure Manual

SECTION 3: SYSTEMS

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Protection of Information	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

PROTECTION OF INFORMATION

POLICY

Mnaasged Child and Family Services will ensure that all service, clinical, financial, or technical information is protected and remains the property of Mnaasged Child and Family Services.

PROCEDURE

1. Employees must maintain confidentiality as outlined in the Human Resources Policy and Procedure Manual: Confidentiality Policy.
2. All Mnaasged Staff have the responsibility to protect the following examples of information regarding Mnaasged and others from illegal, unauthorized, or inadvertent use and disclosure:
    a) Client records
    b) Information contained in business strategies and plans
    c) Pending proposals or contracts
    d) Unannounced services
    e) Research results
    f) Financial data and projections
    g) Proposed acquisitions and divestitures (disposable assets)

3. Information will only be released when it would be in the best interest of Mnaasged and the Clients served by Mnaasged, and in compliance with relevant legislature and Mnaasged's Policy Manuals. Staff disclosing information will require the approval from their immediate Supervisor.

4. Breaches in the privacy and protection of information will be directed to the Employee's Supervisor who will consult with the appropriate Senior Manager.

5. All information stored on servers or network drives will be backed up according to the Backup Policy.

POLICY REFERENCE

Human Resource Policy and Procedure Manual

Department: Information Technology	POLICY #:
Section: Systems	
Subject: User Passwords Credentials	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

USER PASSWORDS CREDENTIALS

POLICY

Passwords are an important aspect of computer security. These are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Mnaasged Child and Family Services' entire network. As such, all Mnaasged Child and Family Services Employees (including contractors and vendors with access to Mnaasged Child and Family Services systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password. The purpose of this Policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this Policy includes all Personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Mnaasged Child and Family Services location and has access to Mnaasged Child and Family Services' corporate network.

PROCEDURE

1. The password used to access Mnaasged's domain and network resources will have a 90-day expiry from the date of creation.

2. Passwords are never to be shared (including email transmission, verbal, text, or any other form of communication) or given to anyone except to the Information Technology Staff if requested.

3. Passwords are not to be written down or stored in plain sight where someone might be able to see or read it.

4. All staff must conform to the noted guidelines listed below in relation to the domain or network password.

    a) Be a minimum length of eight (8) characters

    b) Must include at least one (1) uppercase and one (1) lowercase character

    c) Cannot include the user's first or last name

    d) At least one (1) special character (i.e., # $ %)

    e) May not contain repeating characters (i.e., password)

    f) Cannot be the same password used in 10 previous changes

    g) Passwords can only be reset by the Staff member who initially created the password or by an Information Technology Staff.

SECURITY LOCKOUT

1. A standard account lockout will occur if a password is entered three (3) consecutive times incorrectly. The account will stay locked for a duration of 15 minutes before auto-unlocking occurs.

POLICY REFERENCE

Human Resource Policy and Procedure Manual

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Distribution and Maintenance of Computers	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Regulation 70 https://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900070_e.htm#BK45 CSEC ITSG-06 Communication Security Establishment Canada https://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html	

DISTRIBUTION AND MAINTENANCE OF COMPUTERS

POLICY

The Information Technology Department will be responsible for distributing, maintaining, and safeguarding Mnaasged Child and Family Services Staff computers.

PROCEDURE

1. All laptop or desktop computers will be assigned to Mnaasged Staff by the Information Technology Department and must be used only by Mnaasged Staff for work responsibilities.

2. Upon employment at Mnaasged, the Network Technician will configure a computer system for the new Employee.

3. Computers are purchased from a vendor by Mnaasged with a three-year parts and labour warranty to cover normal operations. Computer equipment will be reviewed yearly to identify when each asset should be replaced. This review will align with an internally developed "hardware lifecycle" practice. This practice will also align with the asset depreciation value as defined by the Financial Policies and Procedures.

4. Staff will be notified of the system refresh procedure(s) when their equipment has been identified for replacement by the Information Technology Department. Definition of the change management related to hardware refresh will be subject to the change based on the environmental variables.

5. If system failures occur due to hardware failure, vendors will be contacted, and warrantied parts will be replaced. If parts are not under warranty, the Systems Administrator will request a quote from the vendors. The quote will be presented to the Director of Finance

and Administration for approval. If approved, a Request for Purchase Form will be completed.

6. If a computer system becomes damaged, it will be reported to the Information Technology Department immediately. A report will be prepared by an Information Technology Staff and forwarded to the Director of Finance and Administration for review and direction. (Please refer to the Human Resources Policy and Procedure Manual: Lost, Stolen, or Damaged Equipment Policy.)

7. If system components are to be upgraded, the Systems Administrator will explore options and provide a quote for upgrades, which will be forwarded to the Director of Finance and Administration for approval. If approved, a Request for Purchase Form will be completed.

8. Computer systems that do not meet Mnaasged standards will be reviewed for removal from Mnaasged Offices. Data from hard drives will be destroyed following Canadian data destruction standards to remove information from the hard drive. Mnaasged will follow the Financial Policy and Procedure Manual: Disposal of Capital Assets Policy for the removal of assets.

9. Mnaasged Staff will report any malfunctions of the computer system to the Network Technicians. If the issue cannot be resolved by the Network Technician, it will be handled by the Systems Administrator.

10. Mnaasged Staff will not install or download any unauthorized software or data. Staff have been granted "Power Users" rights to their computer equipment only. Staff are not permitted to change any local machine settings related to security or software. Any change request items are to be forwarded to the Systems Administrator.

11. Computers will only be repaired or debugged by the Information Technology Department.

12. Mnaasged Staff will be responsible for keeping their computer equipment in good working order. Staff are required to keep their technology visibly clean and free of dust, dirt, and food. Additional cleaning assistance can be requested by Staff to a member of the Information Technology Department.

13. Computers will employ various security and encryption methods that may be subject to change over time.

14. Mnaasged Staff will report lost or theft of computers immediately to the Information Technology Department. The Employee will file a police report immediately upon identification of the loss or theft. This information will be forwarded to their Supervisor, the Systems Administrator, and the Director of Finance and Administration.

POLICY REFERENCE

Financial Policy and Procedure Manual

Human Resource Policy and Procedure Manual

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Distribution and Maintenance of Cellular Phones	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Regulation 70 https://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900070_e.htm#BK45 CSEC ITSG-06 Communication Security Establishment Canada https://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html	

DISTRIBUTION AND MAINTENANCE OF CELLULAR PHONES

POLICY

Mnaasged Child and Family Services has adopted this Policy to govern the use of cell phones in the workplace. This Policy is intended to cover the usage of cell phones only.

The scope of this Policy applies to all Mnaasged Child and Family Services Employees: full-time, part-time, casual, or contractual.

Cellular Plan inclusions will contain the following:

- *3GB Monthly Data Allotment (resets on the 22nd of each month)*
- *Unlimited local and long-distance calling within Canada only*
- *Unlimited text and picture/video messaging*
- *Premium voicemail*
- *Call Waiting, Caller ID, and Conference Calling*

PROCEDURE

1. Mnaasged Staff are required to always keep their cell phone in good working physical condition. Mnaasged Staff are required to always keep their cell phone within the protective case that was issued to them.

2. A monthly data allotment of 6 GB is given on a per-user basis. Data allotment resets on the 22nd of each month.

3. Each mobile device has been programmed by an Information Technology Staff to have the following data notification and limitations set:

    a) 3 GB – Notify Staff that their monthly allotment has reached this data limit

    b) 3 GB – Data is automatically disabled when limit is reached

4. Staff are not permitted to modify any data limits or notifications that have been configured by the Information Technology Staff.

5. If a Mnaasged Employee reaches the 3 GB data limit, the Employee is required to contact an Information Technology Staff member immediately so an assessment of usage can be conducted. If the usage is deemed to be no fault of the Employee, it will be at the discretion of the Systems Administrator to authorize usage beyond 3 GB.

6. Any data overages that occur beyond the 3 GB monthly allotment will be subject to the following:

    a) Immediate assessment of the Employee's cell phone to ensure appropriate data thresholds are set

    b) Review of the Employee's cell phone bill to identify data usage overage for the billing period in question

    c) If usage is deemed as non-work-related by the Systems Administrator, any overages will be billed back to the Employee. The Senior Manager or the immediate Supervisor will be notified of the overage and the course of action that will be taken

7. No calls or text messages outside of Canada are permitted for personal use. All calls made outside of Canada for business must be justified when questioned by the Systems Administrator after a bill review.

8. Any billable usage outside of Canada (text, calls, and data) will be an expense the Employee will be responsible to pay out-of-pocket.

    a) Exception: If an Employee is travelling outside of Canada and is required to be available via their cell phone either through call or text, Mnaasged will incur the associated cost.

9. Subscriptions to any mobile device services that result in monthly overages will be cancelled by the Systems Administrator upon discovery. Any costs incurred to Mnaasged will be billed back to the Employee immediately.

10. Mnaasged Staff are required to always keep a screen lock code on their device. Biometric unlocks are not permitted. A secure 4-digit pin is the only acceptable method of security permitted to unlock the phone.

11. All information contained on the cellular device is considered the property of Mnaasged.

12. Staff are permitted to use their Mnaasged-issued cellular device for personal use.

13. Use of Mobile Phones While Operating a Motor Vehicle (new *Highway Traffic Act* laws as of January 1, 2019):

    a) Mnaasged strictly prohibits the use of cell phones while operating a motorized vehicle while on Mnaasged business. The cell phone usage extends beyond regular hours of operation as Staff may be working overtime, flexing their workday hours, or working on emergency duty.

    b) The suggested practice(s) while driving to make or to receive calls include the following:

        i. Pull over and stop

        ii. Allow a passenger to operate the phone

        iii. Use Voicemail and respond to the call at a safer time

        iv. Let someone else drive, freeing you up to make or to receive calls

14. Employees are solely responsible for any fines or charges laid by the authorities for the illegal use of a cell phone while operating a vehicle during their work hours. Employees who choose to violate the Policy may face disciplinary measures up to termination or may face legal responsibility if, in the course and scope of their duties, they are involved in a motor vehicle accident and there is evidence of cell phone usage while driving, and the employer is sued.

DAMAGE TO THE MOBILE DEVICE

If Employees damage their Mnaasged-issued cell phone, they must take the following steps:

1. Report the incident to an Information Technology Staff member immediately by bringing the device to the closest available office for assessment.

2. The Employee will be asked to fill out the "Cell Phone Damage" Form while the device is being diagnosed by an Information Technology Staff member.

3. After an assessment, a Diagnosis Report will be filed by the Information Technology Staff member.

4. If the device was found to be faulty from the manufacturer, repair or replacement of the device will occur. If the device was found to be handled improperly that resulted in damage, repair or replacement costs *may* be billed to the Employee after consultation with Senior Management.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Internet	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

INTERNET

POLICY

Mnaasged Child and Family Services will ensure that internet access is provided to all Staff and is used for Mnaasged Child and Family Services business purposes. The equipment, services, and technology provided to access the internet will always remain the property of Mnaasged Child and Family Services.

PROCEDURE

1. The use of Mnaasged's "internet" will be primarily reserved for work-related activities. Internet access is the vehicle to the World Wide Web. As such, all activities conducted by Staff on the World Wide Web via Mnaasged's corporate internet is subject to audit. Such examples include, but not limited to, the following:

    a) Social media sites, file sharing, video streaming services, and so on

    b) Staff are permitted to use Mnaasged's internet to conduct personal business that would be deemed work appropriate and safe during breaks or at lunch time. Use of Mnaasged's internet outside of standard business hours is permitted but must adhere to the above-noted safety clause

2. Mnaasged prohibits the use of the internet in ways that are disruptive, offensive to others, or harmful to morale.

3. Mnaasged further prohibits other internet misuse that includes, but is not limited to, ethnic slurs, discrimination, racial slurs, sexual orientation comments, off-colour jokes, religious or political comments, or anything that may be construed as harassment or showing disrespect to others.

4. Internet usage is intended for job-related activities and may be monitored by the Systems Administrator. Reports gathered will be forwarded to the Director of Finance and Administration.

5. The Systems Administrator reserves the right to monitor internet traffic as well as retrieve and read any data composed, sent, or received through Mnaasged's internet data. This information is considered part of the office records of Mnaasged and may be subject to disclosure.

6. A web traffic filtering application will be used to block sites that are not work appropriate. If the situation arises that an Employee requires access to a blocked site, the Employee will contact the Systems Administrator to discuss the need.

7. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the internet is expressly prohibited.

POLICY REFERENCE

Human Resource Policy and Procedure Manual

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Network User Access	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

NETWORK USER ACCESS

POLICY

Protecting access to Information Technology systems and applications is critical to maintain the integrity of Mnaasged Child and Family Services' data and to prevent unauthorized access to such resources. Access to Mnaasged Child and Family Services' systems will be restricted only to authorized users that the Systems Administrator has approved.

The scope of this Policy defines who is permitted access to Mnaasged Child and Family Services' domain and network resources. This Policy also defines how any authorized person(s) will access Mnaasged Child and Family Services network.

PROCEDURE

1. Computers and peripherals that connect Mnaasged's internal network must be owned and centrally managed by the Information Technology Department and must conform to all applicable Information Technology standards and practices. Guest access that has limited connectivity is authorized.

2. No external devices that are not corporately owned and managed by Mnaasged's Information Technology Department are permitted to be connected to any site location's internal network. These devices include, but are not limited to, the following:

    a) Laptops

    b) Desktops

    c) Tablets

    d) Mobile phones and handheld devices

e) Networking equipment

f) Peripherals (printers, scanners, and so on)

3. All domain user and service accounts are stored with Mnaasged's Active Directory. Only authorized Information Technology Staff have access to this application for the purposes of creation, deletion, and suspension of domain accounts in accordance with the policies and procedures contained within this Manual. The Systems Administrator is responsible for all accounts that are created and maintained by the Information Technology Department.

4. For security reasons, all Mnaasged devices will have the USB and CD drives disabled. Account eligibility is at the sole discretion of the Systems Administrator. If a request is placed to have a domain user account created that falls outside of the definition of an Employee of Mnaasged (full-time, part-time, casual, or contractual), the Systems Administrator will request specific details on the reasoning, level of access, and duration of the account. These types of special accounts, if authorized, will be subject to a specific network security control practice that will be defined by the Systems Administrator.

5. User access rights will be adjusted in a timely manner to provide access that is authorized and necessary. This will take place wherever there is a change in business need, a change in position, a change in team assignment, leave of absence, termination, resignation, or retirement. The Human Resources Department will be responsible for communicating any Staff changes that may occur by the end of the business day on each Friday of the month. Communication will be sent using a "Staff Change List" document that will be emailed to all departments. Changes to Staff network access will be completed within five (5) working days of receiving the email communication.

6. Password management will be the domain user's responsibility. Password creation and usage will follow the User Password Policy.

7. Any Employee that holds an active user account but will be on a Leave of Absence for a duration longer than 10 consecutive working days, network account access will be disabled. Leaves of Absence will include, but are not limited to, short-term medical, long-term medical, educational, maternity, paternity, and suspension. The Human Resources Department will notify the Information Technology Department immediately of an Employee's leave and the expected return date.

8. Any domain user account that is disabled for any reason as outlined in clause 7, the user account will be moved to the "Disabled Accounts" organizational unit within the Active Directory indefinitely. Account restoration will occur based on the Human Resources Department's notification of the Employee's return to work date.

9. Under no circumstance will an Employee log into another computer to allow another person(s) to access the network.

10. Failure to comply with any of the above-stated policies may lead to disciplinary action and/or employment termination.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Systems	
Subject: Electronic Data	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

ELECTRONIC DATA

POLICY

Mnaasged Child and Family Services will provide a secure system for the storage of the electronic data of Mnaasged Child and Family Services.

PROCEDURE

1. The Network Technicians will maintain Mnaasged's systems and data and will perform regular backups of all information stored on Mnaasged's servers.

2. The Network Technicians will assist Mnaasged Staff in storing electronic data on network storage to centralize and secure the electronic data.

3. The Network Technicians will create an H:Drive for staff to utilize as their home folder. Staff are to save all documents to this folder. A modified short cut to this network space will be configured on all user machines. Only the individual Employee will have access to this space except for the Network Administrators.

4. The I:Drive is for shared, work-related secure access to electronic data within Mnaasged and can be accessed by all Mnaasged Staff. The folder structure will be defined by teams and locations.

5. The Information Technology Department will ensure that field offices are connected to the network over a secure hardware Secure Socket Layer (SSL) Virtual Private Network (VPN) tunnel connection.

6. The Information Technology Department will ensure that external access to systems will be provided over a secure VPN connection upon a Supervisor's approval.

7. If information is inadvertently removed or missing from a network drive, Mnaasged Staff will contact a Network Technician immediately by telephone or email notification to process a recover or restore from Mnaasged backups if deemed necessary.

8. All documents stored on a network drive will be backed up daily by automated procedures configured and monitored by the Network Technicians.

9. The Information Technology Department will ensure that when an Employee leaves Mnaasged, all documents from the Employee's computer and home drives will be backed up and stored securely on a network drive. These documents may be accessed only by a Senior Manager upon request. This information will be stored for a minimum of six (6) months before it is transferred to another staff or deleted.

POLICY REFERENCE

SECTION 4: MAINTENANCE

Department: Information Technology	POLICY #:
Section: Maintenance	
Subject: Software	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

SOFTWARE

POLICY

Mnaasged Child and Family Services will ensure that all of its purchased software will be installed and maintained by the Information Technology Department.

PROCEDURE

1. When software is purchased for use by Mnaasged, the Systems Administrator will ensure that a backup copy of the software is stored on the server.
2. The Network Technicians will ensure that all required software packages are installed on a staff position basis and configured to align with internal application needs.
3. Staff will only use software approved by Mnaasged for computers and in accordance with the software license agreement.
4. The Information Technology Department will schedule patch management to systems and servers when deemed necessary. Such patch management may require minor disruption in service to Staff, which will be communicated to them prior to deployment.
5. The Information Technology Department will ensure that the software will be configured so that data will be stored on the server, where applicable.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Maintenance	
Subject: Inventory	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

INVENTORY

POLICY

Mnaasged Child and Family Services will ensure that the Information Technology Department will maintain an inventory list of all software licenses and hardware assets.

PROCEDURE

1. When new software or hardware is purchased by Mnaasged, it will be recorded into Mnaasged's inventory software and maintained by the Information Technology Department. Documentation will include serial numbers, part numbers, type of equipment, and warranty status.
2. The Information Technology Department will record in the inventory a list of specialized software installed on end-user machines.
3. The Information Technology Department will record all hardware assigned to Mnaasged Staff.
4. The Systems Administrator will record and sign off on all electronic items designated for disposal from Mnaasged's Computer System Inventory that are slotted for secure destruction.

POLICY REFERENCE

Financial Policy and Procedure Manual

Department: Information Technology	POLICY #:
Section: Maintenance	
Subject: Backups	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

BACKUPS

POLICY

Mnaasged Child and Family Services will ensure that the Information Technology Department will maintain backup procedures within Mnaasged Child and Family Services.

PROCEDURE

1. The Systems Administrator will develop a system backup procedure scheduled to run daily.
2. Full system backups will be stored on a local network storage device located within Mnaasged's Head Office as well as within a cloud-based solution.
3. Incremental backups will run daily and will be stored on a local network storage.
4. Full backups of virtual machines will be completed monthly and will be stored on a local network storage and within a cloud-based solution.
5. In the event of catastrophic hardware failure, the live environment will be switched to the cloud environment until physical systems can be restored.

RESTORATION

1. On a monthly basis, the Network Technicians will test backup procedures by restoring a file from the backup process.
2. If a user reports a missing file, the Network Technician will be contacted, and a restoration of the file will be completed.

3. The Network Technicians will report to the user that the file has been restored and will ask the user to verify the restored contents.

4. The Systems Administrator will test the restoration of full virtual machines monthly.

DATA RETENTION

1. Incremental backups will be maintained for one year before being archived by the Network Technicians.

2. Virtual server backups will only have one copy maintained by the Systems Administrator.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Maintenance	
Subject: Computer Virus	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

COMPUTER VIRUS

POLICY

Mnaasged Child and Family Services will ensure that all computers belonging to Mnaasged Child and Family Services are protected from computer viruses.

PROCEDURE

1. The Network Technicians will install anti-virus software on all Mnaasged computers.
2. The Network Technicians will maintain anti-virus software and will enforce regular updates on all Mnaasged computers.
3. The Network Technicians will respond to virus attacks and will properly remove infections.
4. Incoming media (e.g., floppy disk, USB drive, CDs) will be scanned for viruses before being used.
5. When Mnaasged Staff suspect that their computer has been infected by a virus, they will immediately contact the Network Technicians for further instruction.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Maintenance	
Subject: Access to Servers and Security	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference:	

ACCESS TO SERVERS AND SECURITY

POLICY

Mnaasged Child and Family Services will ensure that servers owned by Mnaasged Child and Family Services are in a controlled and secured environment to prevent damage and other unexpected tampering.

PROCEDURE

1. The servers will be in a locked and temperature-controlled Information Technology room within Mnaasged.
2. The servers will be installed in the server rack along with other devices used for the infrastructure.
3. The server rack will remain closed and always locked. Only the Information Technology Department and the Director of Finance and Administration will have access.
4. Any other devices (e.g., routers and switches) not located within the rack will be secured to prevent removal from Mnaasged's premises.
5. The Systems Administrator will be responsible for accessing server equipment. In the absence of the Systems Administrator, a designate from the Information Technology Department may be requested to access the equipment.
6. If Mnaasged Staff notice that there has been unauthorized access to the server equipment, they are to notify the Systems Administrator and the Director of Finance and Administration immediately.

POLICY REFERENCE

Financial Policy and Procedure Manual

Human Resources Policy and Procedure Manual

SECTION 5: IDENTIFICATION CARDS

Department: Information Technology	POLICY #:
Section: Identification Cards	
Subject: Identification Cards	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

IDENTIFICATION CARDS

POLICY

Mnaasged Child and Family Services will provide Identification Cards to Staff upon employment, which will be created and distributed by the Information Technology Department.

PROCEDURE

1. The Information Technology Department will request and take a picture of the new Employee upon hiring, volunteering, or fulfilling a student placement.
2. The picture will be a centred image of the shoulders and head. Eyes must be open and clearly visible.
3. The front side of the Identification Card will have Mnaasged's full name and logo, the Employee's full name and position, and the date of issue.
4. The back side of the Identification Card will have Mnaasged's full name and Head Office contact information, the Executive Director's digital signature, and a bar code. When the bar code is scanned, it will produce Mnaasged's contact information.
5. Identification Cards do not expire unless the Employee leaves or retires.
6. When exiting Mnaasged, Identification Cards are to be returned to the Information Technology Department.
7. The Information Technology Department will maintain a list of distributed Identification Cards.

POLICY REFERENCE

Human Resources Policy and Procedure Manual

SECTION 6: MNAASGED INFORMATION MANAGEMENT SYSTEM

Department: Information Technology	POLICY #:
Section: Mnaasged Information Management System	
Subject: Case Management	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Regulation 70 https://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900070_e.htm#BK45 *Child, Youth and Family Services Act*, Regulation 206 http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_000206_e.htm	

CASE MANAGEMENT

POLICY

Mnaasged Child and Family Services will use the Mnaasged Information Management System for prevention services, which will be maintained by the Information Technology Department.

PROCEDURE

1. Mnaasged Staff and Supervisors will advise the Information Technology Department of any issues related to the Mnaasged Information Management System.
2. All Mnaasged Staff will advise the Information Technology Department of any perceived security threats or vulnerabilities.
3. The Communication Manager will be responsible for basic maintenance of the website, generating reports, as well as conveying issues to the developers when required.
4. The Information Technology Department will be responsible to assist in training Mnaasged Staff.
5. In a conflict of interest circumstance, the Systems Administrator will implement security measures to restrict Employee access to specified cases in the Mnaasged Information Management System.

6. The Systems Administrator will monitor the security and integrity of data through Audit File Reports and will report any security breaches to the Director of Finance and Administration.

7. The Systems Administrator will participate in Case Management System User Group Service System network of the Mnaasged Information Management System Moderators.

8. The Information Technology Department will configure user account access required by Mnaasged Staff to use the Mnaasged Information Management System.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Mnaasged Information Management System	
Subject: Child Welfare Information Systems (not yet determined)	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: *Child, Youth and Family Services Act*, Regulation 70 https://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900070_e.htm#BK45 *Child, Youth and Family Services Act*, Regulation 206 http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_000206_e.htm	

CHILD WELFARE INFORMATION SYSTEMS (NOT YET DETERMINED)

POLICY

Mnaasged Child and Family Services uses the Mnaasged Information Management System for child welfare matters. The Mnaasged Information Management System will be maintained by the Information Technology Department.

PROCEDURE

1. Helpers will ensure that completed forms are sent to Supervisors for review and approval.
2. Supervisors will confirm and approve all forms from assigned Investigation and Assessment/Child/Family Helpers.
3. Helpers and Supervisors will access the Mnaasged Information Management System database on a regular daily basis to check the Task List.
4. Supervisors will oversee the Helpers' caseloads, including Helper coverage and transfer of cases.
5. Mnaasged Staff will advise the Systems Administrator of computer-related issues with the Mnaasged Information Management System.
6. Mnaasged Staff will advise the Information Technology Department of any security threats or vulnerabilities.
7. The Information Technology Department will configure user account access for Mnaasged Staff to use the Mnaasged Information Management System.

8. In a conflict of interest circumstance, the Systems Administrator will implement security measures to restrict Employee access to specified cases in the Mnaasged Information Management System.

9. The Director of Finance and Administration will respond to the financial requirements in addressing service that is related to the Ministry of Children and Youth Services funding formula.

10. The Systems Administrator will monitor the security and integrity of the Mnaasged Information Management System through Audit File Reports and will report any security breaches to the Director of Finance and Administration and the Director of Services.

11. The Systems Administrator will assist the Finance Department in completing the Days-in-Care process and the validation of data.

12. The Systems Administrator will develop and implement new database forms on the request and approval of the Director of Services.

13. The Systems Administrator will validate the system information and update Supervisors and Senior Management of any incomplete information.

14. The Systems Administrator will generate monthly reports for Supervisors and Senior Management.

15. The Systems Administrator will work with Vertical Software International (VSI) to implement planned software database updates on an ongoing basis.

DATA RETENTION

1. Any case information stored in the Mnaasged Information Management System will not be deleted or removed from the system.

POLICY REFERENCE

SECTION 7: SECURITY OF INFORMATION

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Security of Information	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

SECURITY OF INFORMATION

POLICY

Mnaasged Child and Family Services will ensure that there are security systems in place to protect the integrity of, and access to, all Client files, financial and business records, and all other sensitive information collected by or in possession of Mnaasged Child and Family Services. Access to all information will only be granted to Employees whose duties and responsibilities require access, other eligible persons (Ministry of Children, Community and Social Services representatives; First Nation Band Representatives; and Board of Directors) who are entitled to the information, and Clients who have a concern about their own information. All other access will be provided only with proper consents or where required by law.

PROCEDURE

ACCESS TO SERVICE FILES

1. Access to labelled service files is limited to the Helpers and Supervisor responsible for the file, as well as Staff who have been granted access to the service files (i.e., Program Support, Information Records, Managers, Information Technology, Legal, Director of Services, and the Executive Director).

ACCESS TO THE SERVICE INFORMATION SYSTEM

1. All staff will have access to the Service Information System on a “need-to-know” basis.

SECURITY

1. The Information Technology Department will maintain security profiles as determined by Senior Management to secure Mnaasged data from unauthorized viewing or editing. This will ensure that a user's personal network folder is secured and will only be accessible to that individual as well as the Information Technology Department for maintenance purposes. These security profiles will ensure authorized access to shared network folders.

2. Each application, such as the Service Information System or Payroll, will also have a structured security profile determined by Senior Management within the application that will allow custom security profiles based on the individual's login account. These security profiles will ensure that information within the application is secured with access from authorized individuals only.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Issuance and Replacement of Equipment	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

ISSUANCE AND REPLACEMENT OF EQUIPMENT

POLICY

Mnaasged Child and Family Services provides a variety of office and other equipment to its Employees to be used in the performance of their duties. Some equipment may be issued to Employees upon hiring, and they will be responsible for this equipment while in their possession. Other equipment may be used by all Employees and must be signed out for use and signed in for its return after use.

PROCEDURE

1. Equipment located in an Employee's office will normally be for that Employee's sole use. Shared equipment will usually be placed in common areas to facilitate availability to those Employees using it.

2. Shared equipment will generally stay in one office location. Any Employee using shared equipment will use it on a first-come, first-served basis unless otherwise agreed upon. Equipment may be reserved to ensure it is available when required, using a sign-out system at each location.

3. All office equipment in need of repair or replacement will be reported to the Finance Manager; all computer equipment in need of repair or replacement will be reported to the Information Technology Department as soon as possible.

4. Employees may use equipment for personal use but must sign it out as such and assume the responsibility for any repair or replacement cost for damages incurred while in use for personal reasons. Business use will take precedence over personal use. Equipment used on a personal basis should be returned to the office by the next business day.

5. Unless otherwise directed, Employees will leave all equipment behind when they change positions, teams, or locations to ensure that everyone has the equipment (computer,

telephone, filing cabinet, and so on) needed to do their job. There should always be replacement equipment waiting when an Employee moves to a different or new position.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Service Files and Case Records	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

SERVICE FILES AND CASE RECORDS

POLICY

A Case Record or Service File is created for each family or individual for whom Mnaasged Child and Family Services provides a service. Case records are ordinarily done electronically, although in some circumstances (such as for court purposes) a paper copy may be generated. Whether in paper or electronic form, all service files must be up-to-date, and the information must be verified for accuracy. All service files must be kept confidential and only made accessible to those who are entitled to access the information.

PROCEDURE

REFERENCE NUMBER

1. Every service record will be identified by a unique reference number generated by the Mnaasged Information Management System, followed by the family's or Child's/Youth's name. Once assigned, the reference number becomes a permanent identification number for that family or Child.

CREATION OF SERVICE FILES

1. All services for Families, Children/Youth, and Alternative Care Parents will be recorded and documented in service file records in accordance with Mnaasged Policies as set out in the Mnaasged Service Manuals. This includes recordings of First Response, Child Safety Intervention, Family Care, Children's Care, Alternative Care, Indigenous Knowledge Service, formal Family Circle Gatherings and Circle meetings, Mnaasged Unity Circle meetings, and all related tools and forms that include Mnaasged forms and Ontario Child Protection Tools.

2. All service file recordings will be typed by the Assigned Helper. Printed copies will be maintained in the Family's or Child's/Youth's File.

3. All reports, assessments, plans and other recordings will be reviewed by a Supervisor within the required timelines to ensure that the Helper's work complies with Mnaasged Policies and provincial standards for services and record keeping.

4. All case notes and service file information will be the property of Mnaasged and will form part of Mnaasged's Service File System. The contents of the various service files are detailed in the different Service Manuals. All service file information prepared by the Assigned Helper will be signed (electronically where possible) and dated by the author. The Helper's signature will signify that the facts contained are accurate to the best of the Helper's knowledge and that the stated opinions, assessments, and case plans were provided in good faith and to the best of the Helper's ability.

5. All service file reports prepared by the Assigned Helper will be countersigned (electronically where possible) and dated by the Helper's Supervisor. The Supervisor's signature will signify that the Supervisor has read the report and that it meets Mnaasged and Ministry Recording Standards.

6. When the Supervisor is of the opinion that a service report does not meet Mnaasged or Ministry Standards, the Supervisor will proceed with the following:

    a) If the work is satisfactory other than minor corrections (such as spelling, typing, or grammar errors) the Supervisor may make the corrections, initial them, have the Helper initial the corrections, and countersign the work

    b) If the work requires additions or corrections of a more substantial nature or when there are substantive differences of opinion regarding the Helper's assessments or case plans, the Supervisor may return the work to the Helper unsigned, identify the specific deficiencies, and request that the report be rewritten so that it conforms with Mnaasged Standards

7. Any additions or changes to a service record after the sign-off by the Helper and the Supervisor must be authorized by a Supervisor. Unauthorized changes to a service record will be cause for disciplinary action.

8. If a Supervisor determines that an addition or correction is required for a case file after it having been signed by both the Helper and the Supervisor, one of the following procedures will apply:

    a) Minor corrections such as spelling or grammar errors may be made by the Helper or the Supervisor and initialed by each who signed the original report

    b) Minor omissions may be added by creating a supplementary report, which will be signed and dated by the author and countersigned and dated by the Supervisor, and then appended to the service record

c) More substantial changes may be made by the use of a replacement report complete with a notation about why a replacement report was done, provided that it is completed by the author of the original report, is identified at the bottom of the report as a substitute report noting the date of the original report it is replacing, and is signed and dated by the Helper/author and the Supervisor using the date on which the substitution was approved, and not the date of the original report

FILE RECORDINGS

1. All service records will be completed and maintained in accordance with Mnaasged's format in each service area, as described in the respective Service Manuals. Files will be organized with the use of "File Skirts" for each section of the file.

2. The Assigned Helper will proofread any work typed on the Assigned Helper's behalf, sign, and date the file reports, and submit them to the Supervisor for approval. All Family and Child/Youth information changes will be entered into the Mnaasged Information Management System by the Program Support Staff for the Assigned Helper.

3. The Program Support Staff are responsible to ensure that the file is properly organized, any service reports are printed as required, any updated information changes are entered, and the entire service file is submitted to the Supervisor without delay for approval.

4. The Supervisor will examine the file to ensure that the required services, planning, and recordings have been carried out according to Mnaasged Policies and will sign it once satisfied that these have occurred.

5. If service is to continue for the Family or the Child/Youth, the file will be returned to the Helper after the Supervisor has signed it. If the case is to be transferred to another Helper, the file will be sent to the new Helper.

6. When service is completed for a Family or a Child/Youth, the following procedures will apply.

CONTACT NOTES

1. All Employees having service contact with families, Children/Youth, Alternative Care Parents, community members, and other collateral contacts are responsible to make a written note of their contacts in the Contact Notes. Contact Notes will be recorded as soon as possible and must be recorded within 24 hours after the contact.

2. All Contact Notes will be the property of Mnaasged and form part of Mnaasged's service information.

3. Contact Notes will include the following:

a) Family's or Child's/Youth's full name

b) Date, time, and location of the contact

c) Person(s) involved in the contact

d) Details of what occurred during the contact

e) Personal observations or opinions, as appropriate and identified as such

f) Signature of the author (initials are not acceptable)

g) Date and time that the Contact Note was written

4. All Contact Notes will be compiled on a Mnaasged Form within the Mnaasged Information Management System. Handwritten Contact Notes must be legible.

5. Contact Notes on service files are kept in the case file or in a separate binder of active services. All Contact Notes will be filed chronologically in the service file when the file is being reviewed and when the service is completed.

6. No one will, under any circumstances, alter, edit, or destroy a Contact Note.

SUPERVISORY NOTES

1. All decisions made during a formal supervision session will be documented in the Supervisory Notes. All important decisions made during ad hoc supervision between a Supervisor and a Helper will also be documented in the Supervisory Notes.

2. When a Supervisor is covering for another Supervisor, the covering Supervisor will document all decisions in the Supervisory Notes.

3. Formal supervision for each service is required as follows:

a) Each Child Safety Intervention service will be reviewed by the Supervisor weekly

b) Every Family Care service and service to Children in Alternative Care will be reviewed at least monthly

c) Every Child/Youth in Long-Term Alternative Care will be reviewed quarterly

d) Every Alternative Care Parent Home will be reviewed quarterly

e) Every Family or Child/Youth involved in Indigenous Knowledge Programs will be reviewed quarterly

4. When a Family or a Child/Youth receiving service is not reviewed, the reason will be documented on a Supervisory Note.

5. All Supervisory Note cases will be part of the service record and included in the service file.

6. When service responsibility is transferred from one Helper to another, the Supervisory Notes will be forwarded to the new Supervisor.

7. The Supervisor will document in the Supervisory Notes the date of the last face-to-face contact, the next planned face-to-face contact date, and the planned frequency of the contact.

8. Supervisors will keep Supervisory Notes in binders, separated according to the Families and Children served and the Helper involved. The Supervisory Notes will then be transferred to the file upon completion of the service.

CALCULATION OF DUE DATES

1. In calculating due dates, the day following the date of the initial referral will be counted as "day one." Subsequent dates are calculated from the date of the last completed document of that type; for example, if a report is due every 90 days and is initially completed on the 80th day, the 90 days before the next report begins from the date the report was completed.

AGENCY FORMS

1. For reports and forms that must be completed manually, the respective Program Support Staff will ensure that there are adequate supplies of forms in accessible locations in each office.

2. All forms will be developed on Mnaasged word processing software, unless required to use a government issued or mandated template.

3. All new forms and frequently used older forms should be available electronically in an outline format as well as a hard copy.

4. All Helpers will utilize standard Mnaasged forms that are available either electronically or as a hard copy.

5. All Mnaasged forms must be approved by Senior Management prior to being copied or circulated for use.

SECURITY

1. All service records will be kept reasonably secure from fire, theft, or unauthorized access by any person.

2. All service record files will be maintained in Mnaasged's file room in the central Administration Office. Employees may only access files that are assigned to them. Access to any other file requires supervisory consent.

3. The Employee will be responsible for the security of any files in the possession of the Employee. Service files must be stored in a locked filing cabinet, and all files must be returned to the locked cabinet prior to the Employee leaving the office. The Assigned Helper will lock all service files in the filing cabinet at the end of each business day or lock the office door in which the file is being stored, or both.

4. Service files may be removed from the building for periods of up to two (2) working days with the permission of a Supervisor. Any person removing a file from the building will be responsible for its security.

5. Hard copies of completed service files will be forwarded by the Program Support Staff to the relevant Information Records Staff immediately after the file is completed. Refer to Information Technology procedures for storage of electronic service files.

STORAGE OF FINANCE, PERSONNEL, AND LEGAL FILES

1. Finance files will be maintained in the Finance and Administration Department. Personnel files will be maintained in the Human Resources Department. Legal files will be maintained in the Legal Department.

RETENTION OF RECORDS

1. Except where provincial legislation or regulation dictates otherwise, all inactive service files will be retained indefinitely, either in hard copy or on Mnaasged's laser fiche/electronic information system. Hard copies of files will be destroyed once these are transferred to the laser fiche/electronic information system.

2. Mnaasged insurance contracts will be retained indefinitely. Insurance contracts may be stored off site provided that the required security precautions have been taken.

3. Financial records may be destroyed seven (7) years after the fiscal year in which they were produced, except where retention is required for the purposes of outstanding litigation or where required by law.

4. Duplicate copies of records and file information will be destroyed, as necessary.

LOST FILES

1. The individual who determines that a record is lost is responsible for reporting the loss to the appropriate Information Records Staff and the individual's immediate Supervisor, who will ensure that all necessary activities are undertaken to find the file.

2. If the file is not found after all reasonable efforts have been made to find it, the lost file must be reported to the Executive Director. Mnaasged is then responsible to report the lost file to the Ministry of Children, Community and Social Services and to follow all stipulations under Part X of the *Child, Youth and Family Services Act.*

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Confidentiality	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

CONFIDENTIALITY

POLICY

Mnaasged Child and Family Services is committed to ensuring confidentiality for the Families and Children/Youth using its services. This provision is limited to circumstances where maintaining confidentiality would place a Child or other person at significant risk of harm.

Mnaasged Child and Family Services will respect every person's right to privacy unless it decreases Mnaasged Child and Family Services' ability to protect a Child/Youth.

PROCEDURE

1. "Confidential" means that disclosures made by a person to another in confidence will not be disclosed to anyone else without the person's consent. Exceptions are described below.

2. The following types of information will be considered confidential:

    a) Service information that includes all inquiries, service files, contact notes, agreements, court orders, correspondence, reports and assessments from third party sources, audio or video taped interviews, photographs, or any other personal information that is not public information including verbal disclosures by family members or Children to Employees, Alternative Care Parents, Students, Volunteers, or Board Members.

    b) Mnaasged information that includes the contents of Employee personnel files, personnel matters, finance, property, land, and any matters involving Mnaasged that are being or may be litigated.

3. All persons associated with Mnaasged are responsible for ensuring that confidentiality is maintained in accordance with this Policy and Procedure.

4. Breaches of confidentiality will be considered a most serious performance problem. Failure to comply with this Policy and Procedure will constitute grounds for the removal of a Board Member, Alternative Care Parent, or Volunteer. Non-compliance from Employees will constitute just cause for disciplinary action, including termination.

5. All Mnaasged Employees, Board Members, Alternative Care Parents, and Volunteers will sign a statement acknowledging that they have read and understood this Policy and agree to abide by its terms as a condition of their affiliation with Mnaasged.

6. Accessing and sharing confidential information will be restricted to the smallest number of persons who need to know the information to ensure appropriate accountability, service management, and administration.

7. Clients receiving service, Employees, Alternative Care Parents, Board Members, Students, and Volunteers have a right to access information in accordance with Mnaasged's Policy.

RESTRICTED ACCESS SERVICE FILES

1. Occasionally a service file will relate to an Employee, the Employee's immediate family, or a Board Member. Mnaasged has a responsibility to provide the same degree of confidentiality to such files. At the request of a Supervisor, the information contained within these service files will only be available to individuals responsible for them.

2. A "confidential service file" is designated when access to the record is restricted and the case is assigned as "confidential" status for one of the following reasons:

    a) The person is an Employee or a Board Member

    b) The person is identified as an immediate family member of an Employee (i.e., spouse/partner, children, siblings, parents, grandparents, or grandchildren)

    c) The Executive Director or the Director of Services deems it necessary to designate the file as "confidential"

RECORD CHECKS

1. The First Response Helper or the After-Hours Helper will complete an initial record search in Mnaasged's Information Management System to determine if a Family or a Child/Youth is already involved with Mnaasged services or has been involved in the past. If the record search indicates that the record has been designated as confidential, the First Response Helper or the After-Hours Helper will contact the on-call Supervisor.

RESTRICTED ACCESS FILE IDENTIFIED

1. When a Restricted Access Service File is identified, the file will be moved to the restricted file cabinet within the Executive Administration Office. The Program Support Staff will change the designation of the file in Mnaasged's service information system to "confidential."

2. When a Restricted Access Service is to be provided, the service responsibility may be re-assigned to a different Helper and a Supervisor at the discretion of the Executive Director or the Director of Services.

3. In situations where the Restricted Access Service involves a Board Member, the Supervisor will immediately advise the Director of Services and the Executive Director.

SECURED STORAGE OF A RESTRICTED ACCESS SERVICE FILE

1. The Helper responsible for providing service is also responsible for the secure storage of the confidential service file (both physical and electronic files) throughout the duration of the service.

ALERTS

1. Occasionally, an Alert is filed with the After-Hours Service to provide the After-Hours Helper with critical information about services required after normal office hours. When such an Alert is required on a Restricted Access Service File, the Helper responsible will consult with the Supervisor and the Director of Services to determine how to proceed with the Alert so that restricted information is kept confidential while at the same time ensuring that the Children/Youth are protected.

FILE RETENTION

1. The Executive Assistant will store all Restricted Access Service Files in a restricted locked area in the Executive Administration Office. Any Restricted Access Service File that relates to an Employee or Board Member who is no longer associated with Mnaasged will remain in the Restricted Access storage area.

SPECIAL SITUATIONS

1. If the Executive Director, the Director of Services, the Executive Assistant, or an immediate family member of any of those individuals is receiving service, this person will be excluded from any involvement in the administration or decision making of the procedure for the Restricted Access Service Files.

ACCESS TO RESTRICTED ACCESS SERVICE FILES

1. Access to Restricted Access Service Files in Mnaasged's Information Management System and the actual physical file is granted to individuals responsible for records, the First Response Helpers, the Legal Support Staff, the Director of Services, the Executive Director, and the Helper and the Supervisor providing the service.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Information Disclosure	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

INFORMATION DISCLOSURE

POLICY

Mnaasged Child and Family Services Employees will not disclose any service information to any person, unless it is in accordance with the terms and conditions set out in this Procedure. Guidelines for disclosure of service information will be determined on a case-by-case basis.

PROCEDURE

1. Staff will obtain the family's written consent when requesting information from another service agency or individual, or when releasing service information to another service agency or individual. Exceptions to this may occur when it is part of an investigation and obtaining the information is permitted by law.

2. All persons receiving service will be made aware of their rights and the circumstances under which information must be released without consent.

3. No information, not even acknowledgement, that the person is receiving or has received service will be disclosed to anyone.

4. Service information about a Family or a Child/Youth may be disclosed or released without a signed consent, as in the following:

    a) When a Family or a Child/Youth has moved to another jurisdiction and Mnaasged has referred the matter to the Child Welfare Agency in that jurisdiction

    b) When another Children's Aid Society is providing Child Welfare Services and has requested information compiled on the person(s) by Mnaasged that is relevant to Child protection issues

c) When a Police Officer is executing a lawful search warrant or is jointly conducting a Child Protection Investigation with Mnaasged Staff

d) When a Court has issued an order to disclose the information

e) When persons within Mnaasged's operations need to know the information to provide services, such as Staff, Alternative Care Parents, Volunteers, and Board Members

f) When persons are involved with the following provincial bodies as required under the *Child, Youth and Family Services Act:*

i. Ministry of Children, Community and Social Services

ii. Residential Placement Advisory Committee

iii. Ministry of Children, Community and Social Services Program Supervisor or Review Team

iv. Coroner's Office

v. Courts (in response to a warrant or court order)

vi. Office of the Ombudsman

vii. Office of the Children's lawyer regarding any court action involving Mnaasged

viii. Peace Officer or medical professional if it is believed that failure to disclose is likely to cause the person or another person physical or emotional harm, or if the need for disclosure is urgent

5. Should a service record be subpoenaed to a Court Proceeding or should a Notice of Motion be served to Mnaasged requesting an order to disclose a Mnaasged service file, Mnaasged's Legal Counsel will determine the proper steps.

FAMILY AND CHILD ACCESS TO SERVICE FILE INFORMATION

1. When a Child/Youth or Family has submitted a written request and consent to view the contents of the file, and the request for file information is not court ordered, the responsible Helper (or another Staff person as assigned) will provide the person with a written summary of the contents of the file. The written summary may not include any information pertaining to any other individual for whom Mnaasged has not received written consent to release it.

2. The person providing the disclosure will first read the service record and will then review the nature of the request with a Supervisor to determine what information will be included in the summary report.

INFORMATION DISCLOSED TO THE CHILD'S LEGAL REPRESENTATIVE

1. In the case of a Child/Youth in Care or a Child/Youth brought before the Court as a Child/Youth in need of protection, the consent of the Child/Youth or the Parent(s) is not required for Mnaasged to release information to the Child's/Youth's legal representative.

2. If the Child/Youth is not currently in the Care of Mnaasged and the Child/Youth is not before the Court as a Child/Youth in need of protection, the lawyer will obtain the consent of the Parent(s) in writing for Mnaasged to release information about the Child/Youth and the Family to the Child's/Youth's legal representative, unless a Court Order directs otherwise.

INFORMATION DISCLOSURE FOR CUSTODY AND ACCESS APPLICATIONS

1. In Custody and Access Applications, care must be taken to ensure that information to be shared is only released with the consent of the individuals involved. When such consent has not been received, all information pertaining to the individuals without consent must be excluded from the information that will be shared.

2. Any information in the file that has been compiled by others (e.g., an outside assessment) should be withheld, unless the author has given written consent for its release. It is best for such information to be released directly by the author.

3. Service of a summons does not entitle a party to disclosure prior to a court proceeding. When the summons is directed to the Records Keeper to bring a record, nothing should be provided prior to the Court Hearing and prior to the swearing or affirming of the Records Keeper before the Court and the identification of the said record. All parties must be given an opportunity to object to the release of the contents of the file and to a judicial determination that the record is to be released.

4. The decision on how to proceed in any of the above will be determined by the Director of Services or the Executive Director after consultation with Mnaasged's Legal Counsel.

INFORMATION DISCLOSURE TO OUTSIDE PROFESSIONALS

1. Requests for the release of reports or information by an outside professional for assessment or treatment purposes or for court purposes will be made available only after obtaining the written release from the adult, Parent(s), or Child's/Youth's legal guardian. An exception may be made when a Child/Youth is at risk or the request is the result of a court application by another Children's Aid Society.

2. In all other instances, information will only be disclosed to any other party with the written consent of the person on whom the information has been gathered.

3. The decision on how to proceed in any of the above will be determined by the Director of Services or the Executive Director after consultation with Mnaasged's Legal Counsel.

4. Despite the disclosure provisions of this Procedure, parts of a service file may remain confidential and will not be disclosed if a person or an organization provided information on condition that it be kept confidential and, therefore, Mnaasged kept the information confidential.

5. Confidential information will include written service reports prepared by professionals that have been stamped "confidential" and contain disclosure restrictions. Such information will not be disclosed without the consent of the source of the information or a court order of competent jurisdiction, or if the material is being relied upon in a Child protection proceeding.

6. Depending upon its nature, Mnaasged may resist disclosure of identifying information about Alternative Care Parents, of information that would identify prospective Adoptive Parents, and of material identifying anonymous sources of information (unless under Court Order). No communications between Helpers and Mnaasged's Legal Counsel will be released.

7. Adoption disclosure files will be governed by Ministry legislation, regulation, and policies.

8. Mnaasged may charge a fee for costs associated with copying information for disclosure of information, unless the information is related to a *Child, Youth and Family Services Act* Protection Application currently before the Court, and the recipient is a party to the proceedings.

DISCLOSURE OF NON-IDENTIFYING INFORMATION FOR RESEARCH

Requests for non-identifying service information for research purposes will be made to the Executive Director, who will determine whether the information will be released. The decision will be based on the perceived value of the research and the anticipated costs in Staff time and materials in preparing the information. Costs associated with the information release will normally be borne by the individual or group requesting the information.

AUTHORIZATION FOR RELEASE OF INFORMATION

The Authorization for Release of Information Form is to be used when there is a request for the release of information.

POLICY REFERENCE

Department: Information Technology	POLICY #:
Section: Security of Information	
Subject: Contacts with the Media	
Date Approved:	Date Revised:
Board Resolution #:	
Source Reference: Mnaasged Child and Family Services Internal	

CONTACTS WITH THE MEDIA

POLICY

Only the Board President and the Executive Director are authorized to speak to the media. Specific authorization may be given to Staff to speak to the media on specific occasions and subjects (for example, Alternative Home Recruitment campaigns), and the Executive Director may delegate responsibility to the Director of Services to speak in the Executive Director's absence.

PROCEDURE

PUBLICITY REQUESTS

Whenever information regarding services for Families and Children/Youth is to be used for publicity purposes, the persons involved must give their permission, or the identifying data must be disguised.

COMMENTS ON SPECIFIC PERSONS RECEIVING SERVICE

All requests to comment on a particular situation where Mnaasged is providing service must be directed to the Executive Director. Any comments that will be made will avoid specific references to the Family's or Child's/Youth's situation. General commentary may be made regarding the nature of situations, such as the one being questioned.

FAMILY CONTACTS THE MEDIA

From time to time, a family or a person may approach the media to make their situation made public. All requests by the media to respond to such situations must be referred to the Executive Director. Mnaasged is only permitted to comment publicly on the information

already released, as it then becomes part of the public domain. Responses to criticism should be brief and should focus on the correction of an incorrect impression.

RESPONSE TO PUBLIC CRITICISM

If a formal Mnaasged response is required in the face of major public criticism, the President of the Board and the Executive Director will assess the situation and will then formulate a response. Such statements should be released over the name of the Board President or designate.

REQUESTS FOR INTERVIEWS

All requests by the media for interviews with anyone receiving services, Staff, or Alternative Care Parents must be referred to the Executive Director.

POLICY REFERENCE