**SAFEGUARDS FOR PERSONAL INFORMATION**

**Authority:**

CYFSA – Part X

**Policy:**

Child and Family Services of Grand Erie (the Society) has care of highly sensitive personal information about children and youth, their families, residential care providers, including Customary Care, kin, foster and adoption caregivers, and others. The Society is obliged by law to treat all personal information it holds carefully and protect it. As part of its duties the Society will take steps to keep personal information safe and make sure that it will be accessed only by those who need to see it for a proper reason.

This expectation applies equally to what the Society enters CPIN and other electronic information systems, as well as paper or electronic copies of records, reports, financial records, administrative notes, voice messages, text messages, and emails (including on laptops and cell phones) and any other ways personal information is recorded. The Society must protect this information from loss, theft or unauthorized access including any kind of disclosure to people who should not have the information or obtain information in the wrong circumstances.

**Procedure:**

The Society requires everyone who is affiliated with the organization including all employees, volunteers, foster parents, and students (collectively "Society Members") to follow the best practices described below. Every Society Member has a role in keeping the Society's information secure, and the Society expects everyone to fulfill that role.

**A) Privacy Breach**

All privacy complaints, incidents and actual or potential breaches must be reported immediately to the Society's identified Privacy Lead and Director of Service. The Society will enact the Privacy Breach Protocol Policy.

Types of privacy breaches could include, for example:

- The Society's server is hacked, and personal information is accessed
- A laptop with personal information saved on the hard drive is stolen

- A courier package of service recipient records is not delivered to the correct address
- An unencrypted USB key with service recipient information is lost
- A Society Member talks about a case with a friend and discloses personal information about the children involved
- A Society Member takes a picture or makes an audio or video recording of a service recipient without the knowledge or consent of the service recipient
- A Society Member sends an email that has client information attached, to the wrong email address
- Out of curiosity, a Society Member reviews a neighbour's CPIN person record
- A student looks at CPIN or the electronic information system on a self-initiated education project without being assigned to those cases or people
- A fax with personal information is sent to the wrong number
- A Society Member writes a post on social media about a case with enough detail that the child and/or family would be identifiable to certain people

## B) Restricted Access to Personal Information

Society Members must not access any personal records unless authorized - which means only for legitimate work-related reasons. Society Members may not access CPIN or any other electronic, paper or other records of personal information of their own family, friends, neighbours, or work colleagues unless the Society Member is authorized as part of their official duties (or if covering the shift or tasks for someone who is authorized). Society Members may only access their own personal CPIN or other Society records (if applicable) by making a formal access to records request like any other service recipient.

Society Members must not:

- Access CPIN or other personal information for "self-education" or out of personal interest
- Edit, cut-and-paste, delete from or otherwise change any CPIN or other personal information records except for legitimate reasons. If in doubt or you have questions, always speak with your supervisor first.

## C) Accounts and Passwords

The Society's information technology systems are protected by the use of individual accounts and passwords. Individual accounts are given access to only information required by the account holder.

The Society requires all Society Members to:

- Use only their own user account and password
- Not permit anyone to use their account
- Help maintain security by choosing hard-to-guess passwords
- Contact the Privacy Lead and the IT department, if they suspect any kind of computer access misuse

A good privacy password is a mix of numbers, upper- and lower-case letters and symbols. Avoid using your name or other “easy to guess” words or names in a password. Passwords must be a minimum of eight characters in length. Nonsensical words or a combination of letters and numbers rather than real words or names are suggested. Passwords should not be written down and are not to be shared with anyone.

An unauthorized person trying to gain access to the Society’s IT system or CPIN or other records may not be obvious. Never send your user ID or passwords via email. Never tell anyone your password no matter who they say they are. If anyone you do not know requests information from you, you must verify their identity and their reason for asking, first. If you are left in any doubt contact the IT department.

**D) Physical Security On-Site**

The Society holds a large amount of personal information in printed format - on paper, in files and binders. Schedules and notebooks may also contain personal information.

Access to personal information is permitted by individuals who require the information to complete their authorized work. Service recipients and/or unauthorized people should not be in private areas of the organization. If there is any doubt as to someone's purpose in the building, please contact reception to advise.

Personal information in paper format should be protected from visitors. Personal information not being utilized should be kept in a drawer, cabinet, container or room. Filing cabinets or rooms that contain records should be kept locked unless being utilized.

Where records are on desks in occupied rooms or in paper inboxes they should be turned over (face down) so they cannot be read by someone nearby.

Personal identifiable labels on files should not be visible to visitors.

Personal information that is being stored before secure destruction will be kept separate and clearly marked. Program assistants will identify documents ready for destruction,

place them in containers, seal the container, clearly label the container as “to be shredded” and notify the Property Manager. The Property Manager will store the containers until time of destruction.

### E) Privacy Considerations When Off-Site

Special care should be taken to protect personal information when working off-site or in the community especially in public places. If meeting service recipients in a public place, care should be taken to ensure personal information is not inadvertently overheard or seen by others.

### F) Personal Information in Transit

Because of the serious risk of loss or theft, personal information will only ever be removed from the premises by those Society Members who have a real need to do so to carry out their duties (for example, Society Members who do home visits or transport records to court). This applies to electronic files, paper documentation, paper agendas, and information on laptops, smart phones, disks and memory sticks (USB keys) and any other formats.

Access to electronic files shall be completed through the Society’s remote access via secure server and/or their assigned work laptop. Personal information shall only be stored on portable electronic/devices when necessary to carry out our work. Every time personal information is saved to a laptop, disk or memory stick there is a chance it may be lost or stolen.

When personal information is being taken off-site, it is expected that the Society Member will take steps to ensure the security of the documents. This includes:

1) Where paper documents are necessary, ensuring that the only the necessary documents are being taken off site – rather than for example, the whole file
2) Ensure any portable device and/or paper documentation are always in your control and care
3) Portable devices and/or paper documents are to be transported in the trunk of vehicle where possible
4) Laptops, cell phones, tablets etc. shall not be left visible on the seat of an unattended vehicle at any time
5) No devices or paper documents are to be left in a vehicle overnight
6) Return the device and/or documents to the office building as soon as they are no longer required off site

Personal information relating to Society work should not be stored at home except in very limited circumstances. If the Society Member is required to keep information at home, it must be held securely, and care should be taken to avoid family or friends or other visitors from having any access. Society Members should not make printouts from remote access at home.

All personal information must be returned to the office when no longer required off-site.

## G) Sending/Transmitting Personal Information

Special care must be taken when sending correspondence about a service recipient or that contains personal information, to anyone outside of the Society.

Merely removing a person's name from a record does not necessarily anonymize the record.

### *External Emails and Text Messages*

It may be necessary to communicate with clients and other professionals via electronic means in order to facilitate service delivery. Given the confidential and personal nature of the work done at the Society, it is imperative that electronic communication does not replace vital face-to-face contact.

The Society cannot ensure confidentiality of information shared electronically except for exchanges with other Child Protection agencies. As such, electronic contact should include very limited information from our staff, and all those that we work with need to be made aware of this. We cannot control what a client or other professional includes in electronic contact, however we are responsible for our responses and must ensure they do not contain any identifying, personal or confidential information. Staff should remember that there is no way to confirm who is receiving the information when sent via text or email which could result in a breach in privacy/confidentiality.

Society members will inform clients and other service providers of the risks with regard to confidentiality at the outset of electronic communication. "Guidelines for Using Text Messages" brochures are available for distribution.

Any email with an attachment that contains personal information will only be sent to a recipient that has encryption capability.

Any other information communicated with a service recipient via email or text will be done so on a limited basis and through an approved and secure method. Only the Society email system may be used to send emails to service recipients.

This is important because it:

- Decreases the chance of errors in entering email addresses.
- Ensures that a copy of the email or text is recorded for continuity of service and legal purposes
- Ensures that the email is sent from an approved email address so that automatic reply functionality is working properly
- Ensures that any information not intended for the service recipient is not accidentally sent (such as can be the case with the “reply all” functionality of regular email chains).

If email is to be used for authorized work purposes, the following steps must be undertaken:

- Emails may only include the minimum amount of personal information necessary for the purpose;
- There must be a disclaimer message at the end of the email message being sent (see Appendix A);
- Before sending, the Society Member must check the email address carefully to confirm it is going to the correct recipient (NOTE: email programs that “autofill” the recipient field can insert an address you did not intend to send to);
- The Society Member should avoid using the “reply-all” feature if responding to an email unless applicable and limit the number of recipients to the minimum necessary; and
- The Society Member must check all attachments before sending an e-mail to ensure that the correct document has been attached and no personal information about a different service recipient has been attached in error.

Clients and other professionals should be directed by staff to use the After-Hours Service for urgent matters which arise outside of regular business hours, and not to rely on texting or e-mailing during that time.

Email exchange and text messaging should not be used routinely for communicating with external third parties (for example, other CASs and service providers). Extra care should be used only to include the minimum amount of personal information necessary for the purpose.

In the event of a misdirected email or text containing personal information, it is important to ask the wrong or unintended recipient to confirm that the information was destroyed and not kept or shared with anyone. This should then be documented.

Society Members must report all misdirected emails or texts to the Privacy Lead to ensure appropriate steps have been taken to address the matter and to assess whether a report to the Information and Privacy Commissioner and the Minister of Children,

Community and Social Services is required, as well as notification to affected individuals.

For further information see the Use of Electronic Communication with Clients and Other Professionals – Email and Texting Policy.

***Facsimile (Faxes)***

Misdirected faxes are easy to send and difficult to correct. They make up a significant proportion of privacy breaches. Therefore, when sending personal information by fax, all Society Members should carefully check the fax number - multiple times - to ensure it is correct.

Include a cover sheet stating for whom the fax is intended. The cover sheet must ask a recipient to call if information is received in error.

Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.

After sending a fax, collect and keep a confirmation receipt. If there is any question about a wrong number being used the receipt will make it much easier to check and to retrieve information sent to the wrong place.

A privacy breach occurs whenever personal information is sent to a third party without authorization or without being otherwise permitted or required by law. There can be particularly significant consequences in cases where we repeatedly send service recipient information to a third party improperly.

In the event of a misdirected fax containing personal information, it is important to ask the wrong or unintended recipient to confirm that the information was destroyed and not kept or shared with anyone. Dependent on the situation, we may consider attending to retrieve the information. All activities should be documented in the case file.

All misdirected faxes must be reported to the Privacy Lead to ensure appropriate steps have been taken to address the matter and to assess whether a report to the Information and Privacy Commissioner and the Minister of Children, Community and Social Services is required as well as notification to affected individuals.

If you receive a misdirected fax (meaning you receive a fax that was not intended for anyone at the Society) please notify the sender of their error as soon as you discover it and confirm the fax has been destroyed.  If you notice a pattern of such misdirected faxes received from the same sender in error, please notify the Privacy Lead

### *Social Media*

Society Members will not post any information about service recipient-specific cases online, unless there is a requirement to do so from a court or based on the circumstances to protect a child or as permitted as part of the role of the Society Member. Society Members will also not post comments in internet discussion forums or other online groups that could give the impression of sharing service recipient-specific information.  Even if not referencing individuals by name, extra caution should be exercised when discussing Society work online.

### *Telephone*

Individuals may ask the Society to relay their own personal information to them by telephone. Calling someone at home or at work or leaving messages is an everyday reality that carries a real privacy risk. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, check contact information on a regular basis and ensure telephone numbers and home addresses are accurate and up-to-date. Ask service recipients if messages can be left with someone or on an answering service and clarify the number.

If we have consent to leave a message and you are answered by a machine, listen for clues that you may have misdialed before leaving a message.

If someone calls us, we must take steps to confirm the caller's identity before providing personal information. The Society may accomplish this by asking questions, for example:

- What is your full name?
- What is your date of birth?
- What is your worker’s name?
- When was the last visit?

If speaking on the phone with a child, youth, or family in a place other than the office, Society Members should ensure that no one can overhear the conversation.

### *Mail*

Sometimes it is necessary to send personal information by mail or courier. When sending information in the mail, Society Members will check the address to make sure it is correct. Also, where appropriate, mark the envelope or package "Attention <name>" on the outside to make sure it is opened only by the intended recipient.

Make sure that no personal information can be read through the envelope or window. Correspondence to service recipients will be contained in an envelope that does not have any identifiable markers, such as the Society logo, on it.

For highly sensitive information, a courier service or registered mail is to be considered.

### H) Filing Personal Information

Care should always be taken when tagging and filing electronic records or uploading paper copies of personal information to CPIN and other electronic databases to ensure the information relates to the correct person. Society Members will check names and dates of birth carefully to ensure that files and/or documentation is being stored/added to the correct record.

When personal information is filed in the wrong record, it should be corrected immediately. [NOTE: CPIN does not allow changes to the original record. This is an issue that has been flagged to the Ministry and IPC is aware.] Corrections should be reported to and approved by the Privacy Lead.

If a Society Member finds personal information misfiled in a CPIN case by another CAS, or misfiles information in another CASs record, you must contact the Privacy Lead who will notify the other CAS.

### I) Destroying Personal Information

The Society shall follow its *RETENTION OF VITAL RECORDS AND DOCUMENTS* policy related to the retention and destruction of records.

When material containing personal information is no longer needed, the Society shall ensure that it is destroyed securely as per the following chart:

| Material | Appropriate Method of Destruction |
|---|---|
| Paper (e.g., printouts, faxes, letters, labels, etc.) | Shredding |
| CDs, DVDs, disks, USB keys | Deleting content then shredding or breaking into pieces |
| Audio or video tapes | Erasing content then shredding |
| Pictures, slides | Shredding |

| | |
|---|---|
| Electronic devices with memory storage (e.g., laptops, computers, printers, photocopiers, dictaphones) | Data wiping prior to redeployment or return to vendor – lease company |

Society Members will not recycle any paper or media that contains personal information or treat any paper that has been printed with personal information as reusable for scrap. When personal information is no longer needed, it should be securely destroyed.

### J) Third Party Vendors

When outside contractors attend the Society's offices to perform services/maintenance, they will be required to sign a confidentiality agreement prior to being given access to the building. Contractors will be required to sign a new agreement at minimum annually.

When the Society hires outside contractors to do data entry or provide information systems or to store, transport or destroy personal information, the Society will only utilize those that are bonded and insured and maintain a verifiable commitment to confidentiality. The Society will ensure that the contractor uses the methods documented in the contract the Society has with them.

### K) Breach of Privacy Safeguards

The Society takes safeguarding the private information of those we are engaged with seriously. Failure by Society Members to adhere to the privacy safeguards and guidelines set out above may result in discipline and/or corrective action being taken. Such action may include, but is not limited to: retraining, loss of access to systems, suspension, reporting conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring Society, school or institution, termination of contract, and immediate dismissal. Additional consequences may include notification of affected persons, fines, prosecutions or lawsuits.

This Safeguards policy will be reviewed with all Society staff during orientation and annually thereafter. Staff will acknowledge this annual review via their Annual Declaration.

All volunteers and Society caregivers will review this policy as part of their approval and at Society annual meetings.

## Appendix A – Email Disclaimer Message

“This e-mail message is confidential and is intended only for the persons named above. If you have received this message in error, please notify the sender immediately and securely delete/remove it from your computer system. Any reading, distribution, printing or disclosure of this message if you are not the intended recipient is strictly prohibited. Thank you.”