STATEMENT of POLICY and PROCEDURE			
Manual:	Children First	SPP No.	**ADM 2.15**
Section:	**ADMINISTRATION**	Issued:	**July 22, 2019**
Subject:	**Privacy and Confidentiality**	Reviewed:	
Issue to:	All Manual Holders	Page:	Page 1 of 6
		Supercedes:	January 25, 2019
Issued by:	Executive Director		

STATEMENT:

Children First is committed to respecting the personal privacy of the families with whom we work, our employees, volunteers, donors, Board Directors and any other persons associated with Children First by safeguarding the confidentiality of any personal or identifying information that is entrusted to us, regardless of the format of the information (e.g. verbal, written or electronic). We strive to ensure that the information provided is stored in a safe and secure manner and is destroyed in accordance with relevant legislation.

Personal information is data about an "identifiable individual". It is information that on its own or combined with other pieces of data, can identify an individual[i].

RESPONSIBILITY:

All employees, volunteers, students, Board Members

PROCEDURE:

1. Children First will appoint a Privacy Officer.

2. Children First keeps apprised of privacy issues and ensures that policies and procedures regarding privacy and confidentiality are updated as needed to best protect personal information and to be in compliance with relevant legislation.

3. To emphasize the importance of facilitating the protection, privacy, confidentiality and security of personal information, all new Board Directors, employees, volunteers and students are required to sign a *Promise of Confidentiality* form at the beginning of their involvement with Children First.

4. Children First maintains a Privacy Statement that is made available to all employees, Board Directors and the general public.

5. Children First collects and uses personal information as reasonably necessary to provide quality services, conduct regular business practices, and comply with legal and regulatory requirements. The use of personal information is limited to the purpose for which the information was obtained.

6. Personnel and agents of Children First, as well as accreditors and professional regulatory bodies, are bound by confidentiality with respect to the personal information obtained in the course of their work with our agency. This is effective upon the commencement of their involvement with our agency and continues indefinitely upon their departure.

7. Whenever personal information is requested from or disclosed to other parties, agency procedures regarding informed consent are followed.

8. Children First does not permit identifiable records that are accessed for external purposes (e.g., auditing, licensing, research, or accreditation purposes) to be removed from our premises except as required by law.

9. Personal information may be stored in paper and/or electronic forms. All information is protected by physical and electronic security measures appropriate to the nature of the information and is accessible only by authorized personnel.

10. Children First will utilize physical, technological and administrative safeguards to protect personal information from unauthorized use or disclosure.

11. In the event that personal information has been stolen, lost or accessed by an unauthorized person, follow the procedures outlined below *(Breach).*

12. Children, Families, employees, volunteers and Board Members can request access to, copies of, and corrections to their personal information.

13. Individuals are encouraged to advise us of any changes to personal information that is relevant to their relationship with our agency.

14. Children First will respond promptly when advised that our records are inaccurate or incomplete.

Breach

A privacy breach occurs where personal health information is stolen, lost or if it is used or disclosed without authority.

15. PHIPA requires Children First, as a Health Information Custodian, take reasonable steps to ensure that personal health information in our custody or control is protected against theft, loss and unauthorized use and disclosure, and that the records containing the information are protected against unauthorized copying, modification or disposal.

16. Children First must also take reasonable steps to ensure that personal health information is not collected without authority, and that records of personal health information are retained, transferred and disposed of in a secure manner.

17. Children First may become aware of a privacy breach in a number of ways, including:

    - During the normal course of business.
    - An individual makes a complaint.
    - Notification from the Information and Privacy Commissioner of Ontario (IPC) when a formal complaint has been filed with their office.
    - The IPC initiates its own investigation.

18. Upon learning of a privacy breach, the following steps may need to be carried out simultaneously and in quick succession:

Notification of Staff and Others:

19. Notification of all relevant staff of the breach including the worker's immediate Supervisor, the Program Manager/Administration Manager, the Privacy Officer and Executive Director.

20. A breach or a potential breach[ii] of privacy or confidentiality, including any instance/suspected instance when personal information of an individual who is receiving a service has been collected, used, stolen, lost or disclosed without authority that results in serious harm or risk of serious harm to the individual or others, or is in contravention of Youth Criminal Justice Act (YCJA) is considered a Serious Occurrence (refer to Serious Occurrence reporting policy).

20. The Privacy Officer will **identity scope of breach and take steps to contain it:**

    a. Develop a plan to contain the breach and notify those affected.

    b. Consider whether the nature of the Breach warrants a report to IPC and/or a professional College.

    c. Identify the scope of the breach and take the necessary steps to contain it, including:

        - Retrieve and secure any personal health information that has been disclosed.
        - Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information. Their contact information should be obtained, in the event that follow-up is required.
        - Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. an electronic information system) and take necessary steps, such as changing passwords, identification numbers and/or temporarily shutting system down.

21. Take the necessary steps to notify those individuals whose privacy was breached, including:

    - Identify all affected individuals and notify them of the breach at the first reasonable opportunity. *PHIPA* does not specify the manner in which notification must be carried out. There are numerous factors that may need to be taken into consideration when deciding on the best form of notification, such as the sensitivity of the personal health information.
    - The Privacy Officer will provide direction. For example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at his/her next appointment.

When notifying individuals affected by a breach:

- Provide details of the breach to affected individuals, including the extent of the breach and what personal health information was involved.
- Advise all affected individuals of the steps that you are taking to address the breach, and that they are entitled to make a complaint to the IPC. If you have reported the breach to the IPC, advise them of this fact.
- Provide contact information for someone within your organization who can provide additional information, assistance and answer questions.

Investigation and Remediation:

Children First Executive Director or designate will conduct an internal investigation, including:

- Ensure that the immediate requirements of containment and notification have been met (identify steps taken to investigate this privacy breach and what steps remain to be taken).
- Review the circumstances surrounding the breach.
- Review the adequacy of our existing policies and procedures in protecting personal health information (identify steps taken to remediate and prevent a future privacy breach and what steps remain to be taken to remediate and prevent a future privacy breach).
- Ensure all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of *PHIPA.*

22. The Executive Director will review the information and contact legal counsel when necessary to determine the law(s) that may apply to the potential privacy breach and appropriate measures to respond to the breach.

23. The Executive Director will immediately notify the Board President of any breach with the potential to cause harm to the agency's reputation or other damage.

24. The staff member will immediately complete the *Privacy Breach Incident Form* and forward it to the Privacy Officer. This information will include the following:

- What happened?
- Describe how personal health information came to be stolen or lost or used or disclosed without authority.
- Date (or date range) of theft(s), loss(es) or unauthorized use(s) or disclosure(s) of personal health information.
- Date privacy breach was discovered by the reporting custodian.
- How was this privacy breach discovered by the reporting custodian?

- How many agents of the reporting custodian were responsible, in whole or in part, for causing this privacy breach? Please explain.
- In addition to the reporting custodian, how many other health information custodians were involved in this privacy breach? Please explain.
- Describe the nature of the personal health information that was stolen or lost or used or disclosed without authority?
- The number of individuals whose personal health information was stolen or lost or used or disclosed without authority?
- Were the individuals whose personal health information was stolen or lost or used or disclosed without authority notified of this privacy breach? Including date of notification, by what means, and if not, why not?

25. Upon receipt of the *Privacy Breach Incident Form,* the Privacy Officer will immediately review for completeness and forward the *Privacy Breach Incident Form* to the Senior Management group.

26. The Senior Management team will:

    a. Assess the risk of harm to child/family and the agency if the information is inappropriately used or disclosed (e.g., physical harm, fraud, identity theft, embarrassment, etc.);

    b. Identify the steps that Children First can take to mitigate the effect of the breach and assign responsibility for implementing these steps. This may include recreating the lost information and retrieving copies;

    c. Determine the need for any additional notification strategy for affected individuals;

    d. Determine the need for notification of law enforcement, the IPC or other regulatory authorities;

    e. Develop and implement a communication plan to manage follow-up questions and requests from affected individuals, employees, regulators, law enforcement and the media.

    f. Document plan within two weeks of the date the Privacy Officer became aware of the Breach.

27. In cases where file documentation has been released containing information about another client (e.g., a client's name, address, or other personal health information), the documentation will be managed as per Clinical Record keeping Policy.

28. Depending on the details surrounding the breach, the Human Resource Supervisor in consultation with the Supervisor/Manager/Executive Director will make a recommendation regarding discipline if warranted.

29. Privacy breach incidents will be summarized annually and reported to the Board of Directors and management team.

30. On or before March 1st in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

    1. Personal health information in the custodian's custody or control was stolen.
    2. Personal health information in the custodian's custody or control was lost.
    3. Personal health information in the custodian's custody or control was used without authority.
    4. Personal health information in the custodian's custody or control was disclosed without authority.

31. The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

Cross Reference:
Consents and Authorizations Policy
Consent to Obtain Reference Information
Retention, Disposition and Security of Clinical records
Clinical Record Keeping
Obtaining Informed Consent
Consent for Disclosing or Accessing Personal Health Information
Request for Information Policy
Serious Occurrence Reporting Policy

[i] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[ii] Examples of a breach or potential breach include but are not limited to: a) a staff's laptop is stolen with an individual's files on it, b) a service provider's computer system has been hacked and personal information has been stolen, c) an individual's personal information is posted on social media, d) hard copy materials that contain an individual's personal information are left in a public place.