



## **Privacy of Information Policy**

### **A. Protection of Personal Client Information**

#### **1. Policy**

- 1.01 Brant Family and Children's Services is committed to safeguarding the personal information entrusted to us by our clients. We manage clients' personal information in accordance with Ontario's *Personal Information and Electronic Documents Act (PIPEDA)*, and other applicable laws.
- 1.02 We collect only the personal information that we need for the purposes of providing services to our clients. We inform our clients, before or at the time of collecting personal information, of the purposes for which we are collecting the information.
- 1.03 We collect client personal information directly from our clients or from agencies or individuals that have been authorized by the client to provide us with their personal information.
- 1.04 We disclose client personal information to third parties only with the express consent of the client and only for purposes that have been fully discussed with, and understood by, the client.
- 1.05 We may disclose personal information of clients without consent when required by law, such as when ordered by subpoenas, search or coroner's warrants, or when required to report suspected child abuse to another Children's Aid Society or abuse of an adult with a developmental disability to the Police. In situations where there is a significant and imminent risk of harm to self or others by a client, we reserve the right to notify or respond to authorities or persons at risk.
- 1.06 We may release information without the client's consent as provided in legislation to a Ministry of Community & Social Services or Children and Youth Services employee who is responsible for conducting financial or program audits or study involving the client's record, or for monitoring a program provided by the agency.
- 1.07 A client may withdraw consent to the use and disclosure of personal information at any time, unless the personal information is necessary for us to fulfil our legal obligations. We will respect your decision, but we may not be able to provide you with services if we do not have the necessary personal information.
- 1.08 With respect to the collection of data for files and CPIN, workers will advise that personal information is collected for a provincial database according to the service agreement for CPIN.
- 1.09 We shall ensure that this policy is provided to all persons receiving service or support and that it is presented in a language and manner, and with a level of support, that is appropriate to the capacity of the person, and any person acting on their behalf.

1.10 The Privacy Manager is accountable for the implementation of this policy. Any issues, questions or complaints arising from breaches of this policy should be directed to the Privacy Manager.

## **2 PURPOSE**

2.01 The purpose of this policy is to preserve the privacy of clients of the Brant Family and Children's Services, by outlining employee obligations and procedures for dealing with personal, privileged and/or confidential client information.

## **3 SCOPE**

3.01 This policy applies to all employees, students, volunteers, contractors, subcontractors of Brant Family and Children's Services or anyone else who is granted access to personal, privileged and/or confidential client information.

## **4 RESPONSIBILITY**

4.01 Employees are responsible for:

- being familiar with and following policies and procedures regarding the collection, use, disclosure, security of and access to client personal information;
- obtaining the proper consents and authorizations prior to the collection, use or disclosure of personal, privileged and/or confidential information except where permitted or required by law;
- immediately reporting any breaches of confidentiality to their Supervisor;
- reviewing this policy with clients and ensuring that it is presented in a language and manner, and with a level of support, that is appropriate to the capacity of the person receiving services or support, and with any person acting on their behalf;

4.02 Supervisors are responsible for:

- orienting new employees, students and volunteers to the Client Personal Information Policy and having them sign the Confidentiality Form;
- ensuring that employees, students and volunteers receive an annual refresher on the Client Personal Information Policy;
- ensuring that appropriate client consents are obtained for the collection and disclosure of personal information from or to a Third Party;
- ensuring policies and procedures regarding collection, use and disclosure of personal information are consistently adhered to;
- cooperating with the Privacy Manager to investigate complaints or breaches of policy;

4.03 The Privacy Manager is responsible for:

- ensuring internal compliance with applicable policies or legislation;
- ensuring that all policies related to the protection of personal information are reviewed on an annual basis, and updated as necessary;
- notifying individuals and following the procedure for situations when personal information has been released without prior consent or where records are lost, stolen or destroyed;

- responding to concerns or questions about the Client Personal Information Policy and to complaints about breaches of the policy.

## 5 DEFINITIONS

- 5.01 "**Personal information**" is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to any detail of services or supports received from Brant Family and Children's Services, or from any other service provider.
- 5.02 "**Third parties**" are individuals or organizations other than the subject of the records or representatives of Brant Family and Children's Services

## 6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

- 6.01 *Personal Information Protection and Electronic Documents Act (PIPEDA)*  
*Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008 Ontario Regulation 299/10 Quality Assurance Measures*

## 7 PROCEDURE

- 7.01 Before or at the time of collection, employees will provide each client with an explanation as to why their personal information is being requested and how this data will be collected, used and disclosed. Employees will ensure that the information is presented in a language and manner, and with a level of support, that is appropriate to the capacity of the person receiving service or support, and with any person acting on their behalf.
- 7.02 After providing this information, the client's written consent or the written consent of their substitute decision-maker may be obtained by using the Consent to Release Information *to/from* the Brant Family and Children's Services, Attachment C to this policy. This consent form must bear the client's name, the employee's name and name of the organization, the name of the person or organization to which the information is being released, the specific information being released and the date of the consent. The purpose of the release of information will be documented in the client's file and the client will check off on the release form that he/she understands the purpose for the release. A copy of the release will be kept in the client's file. If the information needed pertains to a couple or a family, each individual over 16 years of age must sign the consent form. If the client is under 16 years of age, authorization for release of information must be signed by a parent or guardian. An authorization for release of record information is valid for the period of time specified on the consent.
- 7.03 Client requests for disclosure of their own personal information to Third Parties must be accompanied by a completed signed and dated Consent to Release Information form.

- 7.04 Clients may withdraw their consent for the collection, use or disclosure of their personal information at any time by notifying the employee. Withdrawal of the consent has no effect on information that has been already collected, used or disclosed before the client withdrew consent. If the withdrawal of consent will compromise the services being delivered to a client, the employee should discuss the effect of the withdrawal with the client and document the withdrawal and these discussions in the client's record.
- 7.05 When clients request a copy of their records, employees will obtain the client's signed consent by completing the Consent to Release Information and place it in the client's file. The staff person will inform his/her Manager about the request. The Manager will review the file to screen for inappropriate file information or information about a third party where third party authorization has not been granted or where there is information contained in the file that serious harm is likely to ensue if access to this information is granted. The Manager will remove the third party reports contained in the file. The Manager will make an appointment with the client to review their record with the staff person present if the client prefers. The client may request a correction of information contained in the file. Given that the original record cannot be corrected in Caseworks, an activity note is entered in the client's file indicating the request for a change and noting what information was amended. The activity note will also include what information was copied, and released, the date the copy was released, the party to whom the copy was released and the person who released the copy.
- 7.06 The Privacy Officer will personally contact a client whose personal information has been used or disclosed without their written consent or where it has been stolen or lost. An investigation will be conducted by the Privacy Officer with the aim of recovering the stolen or lost information and a review of the circumstances that led to the misuse, release, theft or loss of the personal information. The investigation may result in disciplinary action of employees, students or volunteers up to and including termination of employment or contract. In the case of theft of personal information, the Police will be notified. The Privacy Officer will implement any changes to the policy and procedures required to avoid a re-occurrence of the events.
- 7.07 Unless retention of personal information is specified by law or best practice for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.

## **8 ATTACHMENTS**

Attachment A - Confidentiality Form – Employees, Students and Volunteers

Attachment B – Confidentiality Form – Contractors, Visitors and Guests.

Attachment C - Consent to Release Information



## **Privacy of Information Policy**

### **B. Personal Information Protection**

1. Brant Family and Children's Services is committed to protecting the privacy of its employees, clients and others for whom the agency may collect personal information for specific purposes.
2. Employees are obligated to ensure that personal information, to which they may have access remains confidential, is only used for the purposes for which it was collected, is not used for personal gain or disclosed without authorization.
3. Employees, students, volunteers and others who are authorized to collect personal information on behalf of the agency, including persons completing third party audits, or persons conducting reviews on behalf of accrediting bodies or legally authorized funding bodies, are bound to sign a Confidentiality Form – Attachments A and B - indicating that they understand and will respect the privacy of clients, employees, students and volunteers and will hold in confidence all professionally acquired information. This statement shall be retained by Brant Family and Children's Services, for the duration of employment or contract, or for the duration of a specified purpose, such as audit or accreditation or program review
4. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
5. Employees, students and volunteers are required to follow all procedures regarding collection, use, disclosure, security of and access to personnel, client, corporate and financial records.
6. Employees, students and volunteers who disclose information contained in client, personnel, corporate or financial records or place the security of these records at risk contrary to this policy will be subject to disciplinary measures, up to and including termination for cause or termination of student placement or volunteer assignment.
7. The Privacy Manager is accountable for the implementation of this policy. Any issues, questions or complaints arising from breaches of this policy should be directed to the Privacy Manager.
8. Individuals and members of the general public can obtain information about the Personal Information Policy from the Brant Family and Children's Services employees and postings in its offices and on its website.

## **2 PURPOSE**

- 2.01 All employees, students, volunteers, and others who are authorized to collect personal information on behalf of the agency may receive personal, privileged and/or confidential information concerning other employees, students or volunteers, agency operations, clients or others with whom the Agency conducts

business. The purpose of this policy is to preserve the privacy of those parties and Brant Family and Children's Services, Inc., by outlining employee obligations and procedures for dealing with personal, privileged and/or confidential information.

### **3 SCOPE**

3.01 This policy applies to all employees, students, volunteers, contractors, subcontractors of Brant Family and Children's Services, or anyone else who is granted access to personal, privileged and/or confidential information.

### **4 RESPONSIBILITY**

4.01 Employees, students and volunteers are responsible for:

- being familiar with and following all policies and procedures regarding the collection, use, disclosure, security of and access to personal information;
- obtaining the proper consents and authorizations prior to the collection, use or disclosure of personal, privileged and/or confidential information except where permitted or required by law
- immediately reporting any breaches of confidentiality to their Supervisor;
- adhering to the safeguard measures that protect the storage, security, access to and destruction of personal information
- relinquishing any personal, privileged, confidential or client information, keys, laptops, phones or other agency equipment in their possession before or immediately upon termination of employment.

4.02 Supervisors are responsible for:

- familiarizing new employees, students and volunteers to all policies related to the protection of personal information
- ensuring that a valid Confidentiality Form has been completed and is kept on file for new employees, students and volunteers
- ensuring policies and procedures regarding collection, use, disclosure of personal information and access to and security of records are consistently adhered to;
- responding to requests for disclosure after the proper release is obtained;
- cooperating with the Privacy Manager to investigate complaints or breaches of policy;
- obtaining from employees prior to their termination any personal, privileged, and confidential or client information, keys, laptops, phones or other agency equipment in their possession.

4.03 The Privacy Manager is responsible for:

- familiarizing new Board Members to the Personal Information Policy and having them sign the Confidentiality Form;
- ensuring internal compliance with applicable policies or legislation;

- engaging with supervisors, human resources and/or payroll personnel in developing internal policies for the collection, use, and disclosure of personal information and the access to, storage, retention and destruction of personnel, client, financial and corporate records;
- notifying individuals and following the procedure for situations when personal information has been released without prior consent or where records are lost, stolen or destroyed;
- responding to written concerns or questions about the Personal Information Protection Policy and to complaints about breaches of the policy.

## 5 DEFINITIONS

- 5.01 "**Personal information**" is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title, business contact information or job description.
- 5.02 "**Students**" are individuals who are performing unpaid workplace internships or assignments under a student placement agreement between a recognized post-secondary institution and Brant Family and Children's Services.
- 5.03 "**Volunteers**" are individuals who are performing unpaid workplace activities, as directed by a Program Manager, as part of a volunteer agreement between the individual and Brant Family and Children's Services.
- 5.04 "**Third parties**" are individuals or organizations other than the subject of the records or representatives of Brant Family and Children's Services. Note that in certain circumstances, the agency may be entitled to provide personal information to an external party acting as an agent of Brant Family and Children's Services.

## 6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

### 6.01 *Personal Information Protection and Electronic Documents Act (PIPEDA)*

Protection of Personal Client Information

Protection of Personal Employee Information

Third Party Reference Requests

E-Mail and Internet Use as found in the agency's IT Manuals

Remote Access

Social Media

## 7 PROCEDURE

- 7.01 The Agency shall ensure that all new employees, students, volunteers, and others who are authorized to collect personal information on behalf of the agency, including persons completing third party audits, or persons conducting reviews on behalf of accrediting bodies or legally authorized funding bodies, shall complete a Confidentiality Agreement prior to the beginning of their employment, student placement, volunteer assignment or any activity that will allow access to personal, private or confidential information of employees, students or volunteers, agency operations, clients or others with whom the Agency conducts business.
- 7.02 The Agency shall ensure that signed confidentiality agreements will be kept in secure personnel or business files.
- 7.03 Supervisors shall ensure that all new employees, students and volunteers have reviewed relevant Policies and that they understand their contents, prior to their gaining access to the personal, privileged and/or confidential information concerning other employees, students or volunteers, agency operations, clients or others with whom the Agency conducts business.

### 7.04 Safeguards

#### 7.04.1

- (a) The nature of security safeguards shall be determined by and proportional to the sensitivity of the personal information involved. When determining the level of sensitivity of personal information, two factors will be taken into account:
- The quantity of personal information that may be revealed, if accessed by an unauthorized party and
  - The magnitude of potential harm that an individual may suffer, should his personal data be misused or disclosed in an unauthorized manner.
- (b) Client, employee, financial and corporate records are the property of Brant Family and Children's Services and will be stored securely, protected against loss, theft, tampering, copying or access by unauthorized persons. Client, employee, financial and corporate information is only to be accessed by employees with appropriate authorization. No amendments will be made to any part of a record, after it has been initialled.
- (c) Physical measures (locked filing cabinets and offices, restricted access to office, security alarms, etc.), organizational measures ("need to know access", staff training, confidentiality agreements etc.) and technological measures (passwords, encryption, firewalls) are used to safeguard personal information, as appropriate.
- (d) Hard copies of client records will remain on the premises of Brant Family and Children's Services unless a Manager, due to exceptional circumstances, approves removal. If a file is removed from the office for any reason, the name and file number of the file must be registered in writing with the appropriate unit manager or his/her designate. Likewise,

files returned to the office must be registered as having been returned. No client file is to be left in an unlocked vehicle or visible in a locked vehicle; all client files are to be secured when at the employee's home or an alternate location.

- (e) Employees who are approved for remote access must have remote connectivity set up and initialized by the agency's IT service provider. If deemed necessary by the employer, specific equipment for connecting to the network will be provided to the employee. All forms of remote connectivity to the agency's network other than those initialized by the IT service provider are strictly forbidden.
- (f) Electronic Information is subject to the same security as written information and must be accessible to any individual or family. The Agency is the sole proprietor of computerized client or Agency data. Computerized information used or maintained to facilitate information exchange in support of client care shall be accessible only to authorized persons and password protected. Computerized data shall be protected so that it cannot be altered or purged without the proper authorization.
- (g) Access to agency on-site servers and unassigned computer equipment must be locked and controlled.
- (h) Terminals must be located in such a way that the screen cannot be viewed by unauthorized persons.
- (i) All employees are prohibited from storing client information or proprietary agency information on personal computers.
- (j) Electronic client files. Backups are to be performed daily and routine maintenance and review of security protocols are to be performed.
- (k) Files will be accessible by agency personnel via dedicated remote connection. Back-ups are to be performed daily and routine maintenance is to be done on a regularly scheduled basis. Security protocols are to be reviewed and updated on a regular basis.
- (l) Database or system breaches and/or security threats are to be reported to the Privacy Manager (currently the QA Manager) or designate, immediately. In such cases, a threat assessment and action plan will be developed in conjunction with IT and reported to the Executive Director.
- (m) All client records which are not required by the government to be retained indefinitely, are retained for a period of seven years and are routinely destroyed as soon after expiration of the required period as practical. If destruction is performed by a third party contractor, signed confidentiality agreements shall be obtained from all contractor employees who perform the destruction of the records.
- (n) The Director of Administrative will organize the preparation of personal information destruction. Physical records will be destroyed by shredding. If shredding is performed by a third party contractor, signed confidentiality agreements shall be obtained from all contractor employees who perform the destruction of the records. Electronic records will be destroyed by

permanent deletion and will be performed by the agency's IT contractors, or contracted database managers.

7.03 No employee, student or volunteer shall be disadvantaged or denied any benefit of employment by reason that Brant Family and Children's Services believes that they will do anything referred to in paragraph (a), (b) or (c) below or by reason the employee, student or volunteer acting in good faith and on the basis of reasonable belief:

- (a) disclosed to the Privacy Commissioner of Canada that Brant Family and Children's Services or any other person has contravened or intends to contravene a provision of PIPEDA related to the protection of personal information;
- (b) has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA related to the protection of personal information;
- (c) has done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA related to the protection of personal information not be contravened.

## **8 ATTACHMENTS**

Attachment A - Confidentiality Agreement – Employees, Students and Volunteers

Attachment B – Confidentiality Agreement – Contractors, Visitors and Guests

Attachment C - Consent to Release Information



**Appendix A**  
**CONFIDENTIALITY AGREEMENT**  
**EMPLOYEES, STUDENTS AND VOLUNTEERS**

I, \_\_\_\_\_, understand that I may come in contact with confidential information during my time at Brant Family and Children's Services (the Agency). As a condition of my employment, student placement, or volunteer assignment with the Agency, I hereby undertake to keep in strict confidence any information regarding any client, employee or business of the Agency, or any other organization that comes to my attention while at the Agency. I will do this in accordance with the Agency's privacy policy and applicable laws, including those that require mandatory reporting.

I also agree to never remove any confidential material of any kind from the premises of Brant Family and Children's Services unless authorized as part of my duties, or with the express permission or direction to do so from the Agency.

I understand that breach of this agreement will result in disciplinary action, up to and including termination of my employment, student placement or volunteer assignment.

\_\_\_\_\_  
(Print Employee/Student/Volunteer Name)

\_\_\_\_\_  
(Signature of Employee/student/Volunteer)

\_\_\_\_\_  
(Signature of Witness)

Dated this \_\_\_\_\_ day of \_\_\_\_\_, 2\_\_\_\_\_



## Appendix B

### **CONFIDENTIALITY AGREEMENT CONTRACTORS, VISITORS AND GUESTS**

I, \_\_\_\_\_, understand that I may come in contact with confidential information during my time at Brant Family and Children's Services (the Agency). I hereby undertake to keep in strict confidence any information regarding any client, employee or business of the Agency, or any other organization that comes to my attention while at the Agency.

I also agree to never remove any confidential material of any kind from the premises of Brant Family and Children's Services unless authorized to do so by written agreement with the Agency, or with the express permission or direction to do so from the Agency.

\_\_\_\_\_  
(Print Name of Contractor/Visitor/Guest)

\_\_\_\_\_  
(Signature of Contractor/Visitor/Guest)

\_\_\_\_\_  
(Signature of Witness)

Dated this \_\_\_\_\_ day of \_\_\_\_\_, 2\_\_\_\_\_



## Appendix C

### CONSENT TO RELEASE INFORMATION

I \_\_\_\_\_ agree that an authorized representative of Brant Family and Children's Services:

May release information to:

May gather information from:

\_\_\_\_\_  
Name of agency

\_\_\_\_\_  
Address

I have agreed to the release of the following:

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Description of information to be released and purpose for release (including any specified limitations)

This Agreement ends on the earlier of, \_\_\_\_\_, or one year from the date of signature.

I understand the nature and purpose for which my confidential information will be released and give my consent voluntarily.

\_\_\_\_\_  
Signature of Client or Legal Guardian

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Brant FACS Authorized Representative