Boys and Girls Clubs of the Foothills

Privacy Policy and Procedure Manual

Boys and Girls Clubs of the Foothills

Great futures start here

Approved: January 26, 2011, October 26, 2016, September 18, 2019

Policy:
The BGCF will protect the privacy and maintain the confidentiality of its employees, contract workers, members, clients, donors and stakeholders.

Guiding Principles:
The BGCF Privacy and Confidentiality Policy exists in order:

- to support policy formation and managerial decision making
- to improve client services, to support consistency, continuity and productivity in
- operations
- to protect the interests of the organization and the rights of clients, the public and
- employees
- to provide protection and support in litigation, including management of risks
- to facilitate research and development
- to enable the organization to meet legislative and regulatory requirements.

Cross References:
FOIP Act, Information Request Form, Confidentiality Agreement, Release of Confidential information, Reference Permission Form

Procedures:
Definitions:

- Personal Information: Any information that can be used to distinguish, identify or contact a specific individual. This information can include an individual's opinions of beliefs, as well as facts about or related to the individual. Examples include age, marital status, address, and opinions about someone. Exceptions include information that is available to the public such as telephone numbers and addresses as published in telephone directories. This also includes information that is organized by the name of an individual, symbol or other particulars that are assigned to an individual.
- Record: A document containing identifying information in any form including drawings, letters, photographs, and papers that are written, photographed and stored in any manner, which does not include software or other mechanisms which produce records (FOIP Act).
    - Transitory Record: A record in any media that has only temporary usefulness, is not part of a records series, is not regularly filed in a record information system and is only required for a limited period of time for the completion of a routine action or the preparation of a record. This includes, but is not limited to, telephone messages, calendars, informal notes, electronic mail, and drafts of correspondence and reports. Process notes are not considered transitory records and will be kept in the individual's file.

Collection of Personal Information:
The Agency will collect information for program operations and activities of the Agency

and for no other purposes. Any collection of personal information will be useful for the purpose of offering services, maintaining accountability, program purposes, supervision and continuity of services.

The individual and/or their legal guardian, when possible, will consent to information collected. Documentation must:

- be factual
- be objective, reflecting a high degree of professional judgment
- avoid unrelated, non-relevant information
- not include personal comments and opinions
- collect any information necessary to provide appropriate services
- state client opinions if different from the employee or service provider
- be kept for at least one year after using it. This time period may be decreased if both the agency and the individual mutually agree. The decision to destroy records must be approved by the Privacy Officer, program supervisor and C.E.O..
- identify dates and persons as clearly as possible
- include only information that is necessary to provide services to the client
- avoid duplicate material on record

Use of Personal Information:

Employees, Service Providers and Volunteers:

- Employee/service provider/volunteer information cannot be used for purposes other
- than intended.
- The Agency can give reference information to any prospective employer only if the
- employee/service provider/volunteer consents and may only disclose information the
- employee/service provider/volunteer has specifically consented to being disclosed as
- per a completed reference permission form.

Clients:

Personal information is to be used only for intended purposes such as continuity of care, supervision and case planning. Staff must obtain appropriate consents for any new purposes, such as information sharing.

Written consent shall be obtained from the client (or legal guardian) before any communication or information is obtained from the client (or legal guardian) before any communication or information is obtained from or released to any other organization or individual not employed by the Agency. If clients or participants request that information be shared, they must complete a Release of Confidentiality Information Form. This form must specify the following information:

- with whom the information will be shared
- for what purpose
- for how long the consent will remain in effect
- the form must also include a signature and date of signature
- if required, witness signature and date of signature

Client information or communications may be shared within the Agency only with staff involved with a particular client.

Client information to be obtained or released shall be directly related to delivery of services, determination of needs or a mutually defined purpose as agreed upon by the client (or guardian) and the service provider.

All employees, volunteers and contract workers will preserve confidentiality with respect to any identifying information of any person. Do not include other clients, friends or family members in any services provided without the consent of the client. If there are individuals present, their presence must have a direct relationship to the client achieving their goal(s).

If a client has not consented to release information, client information or records, will not be released unless subpoenaed, the client poses harm to him/herself and /or others, or there are child protection concerns.

Staff shall testify in court in regards to client information only if he/she is subpoenaed.

Exceptions:

- Contacting emergency services for the safety of an employee/service provider/ volunteer or client will not constitute a breach of confidentiality.
- Where the employee/service provider/volunteer or client is known to be engaging in activities where he/she is a threat to him/herself or another individual, is abusing, neglecting or putting a child at risk, staff shall document concerns and report the activities to the appropriate agency (RCMP, Children's Services, etc.).
- If the Privacy Commissioner requests information, a release of information is not needed and the Agency must comply with the request.

Information Requests:

There are three types of requests: personal, general and corrections.

Personal Requests:

Personal Requests are those involving personal information about an identifiable individual. All clients and their guardians, employees and volunteers have the right to access their personal information/records in accordance with FOIP.

Requests for access to records will be made in writing by completing an Access to Information Form. The applicant must provide enough detail on the form in order to identify the record. If assistance is needed to complete the Access to Information Form, this can be provided to the applicant.

- The agency will make every reasonable effort to respond to a request no later than thirty (30) days after receiving it.

- If additional time is required to produce a record for a request a reason in writing will be provided to the individual making the request.
- The applicant may ask to view the record or ask for a copy of the record. For all copies, the applicant will be charged a fee of $0.25 per page.
- An applicant may request the Information and Privacy Commissioner to review any decision made by the Agency that relates to a request.
    - The Agency may make copies of the requested record if records are submitted to the Privacy Commissioner and it is anticipated that the information may be needed.
- If there is involvement with Children's Services, Case Workers and Supervisors will have access to client files and information with the consent of clients. Requests for access to records by clients made to a Case Worker will be passed on to the Privacy Officer who will then block information relating to third parties in accordance with FOIP. If the process is complex the file may be passed onto the Privacy Commissioner to process the access request.
- All access requests made on closed files will follow the same procedures for active files.
- If there are multiple clients assigned to a file (couple/family) then consent must be signed by all parties in order to access the complete file. If all parties do not give consent, then the client may see portions of their file, which do not refer to other clients. Information relayed by third parties may be blocked.
- If the Privacy Commissioner requests records, the Privacy Officer at the Agency will state any concerns about releasing the information (if applicable). Concerns may include that the record contains information that is an invasion of another person's privacy; releasing information may cause harm or threaten the safety (emotional or physical) of someone else (this must be in the opinion of a psychologist, psychiatrist or a physician).
- Employees or volunteers may access their record of personal employment by making a verbal or written request to their supervisor. All information, with the exception of confidential information collected during reference checks will be provided.
- If there are informal files on employees that are separate from personnel files, employees also have access to all information contained in this file.
- Job applicants can see all of their personal information, provided that information about other candidates is severed from the record. Other information that could be disclosed includes factors such as ratings and rankings provided that no other personal identifiers are disclosed.
- Applicants may request to view any notes that were made by interviewers.

<u>General Requests:</u>

General requests are those relating to activities of the Agency. Examples include requests for a departmental survey, salary scales, job descriptions and financial reports.

- All general requests will be considered after an Access to Information Form has been completed.
- All requests must be specific as to correctly identify the record.

- If the access request is denied the individual may make a request to access the records through the Privacy Commissioner.

Correction Requests:
Correction Requests are requests for the correction of an omission or error in documentation.

Clients, members, participants, volunteers, contracted staff and employees have the right to request a correction of information if there is an error or omission in information.

- Corrections and correction notices will be completed within 5 days of the correction request. Exceptions to the correction request include professional opinions and must be corrected.

- If the Privacy Officer refuses a correction request, the information in question will be linked to the correction request for future reference.

- Notification of other parties who have had access to the incorrect information in the previous year will occur, unless the change is not material or the individual agrees that it is not necessary.

- If the person requesting the correction request is unsatisfied with the correction or decision of the Privacy Officer to not complete a correction, the individual may contact the Privacy Commissioner.

Records Management:
The Agency will maintain a records system, which may be computerized or manual, which captures, maintains and provides access to records over time.

Manual records include insurance documents.

Electronic records include electronic documents, such as word-processed documents, e-mail, web pages, graphics, digital photographs, and scanned images; and electronic data, such as information stored in databases. They include information in all media and in all locations. For example, electronic records may be stored on networks, local hard drives and portable hard drives, as well as in storage media such as portable disk drives, CD-ROM disks, optical disks and tape.

Non-transitory (permanent) records in the form of electronic documents will be printed and managed as part of the record-keeping system applied to hard copy records. Once a hard copy exists the electronic copy will be deleted.

The Agency will create records only to operate its program and services and will not produce information that is not required.

The Agency will maintain a records system in order to identify, locate and produce records in response to information requests. This system may be maintained by individual programs.

All files are archived to the File Storage Room indefinitely; after the life of the BGCF ceases to exist.

All records will be stored in a secure location, which will not be accessible to individuals other than staff.

Certain types of recorded information are generally managed as transitory records which have only short-term value and may be disposed of regularly at the discretion of an employee:

- information of short-term value (e.g. Notes kept to prepare official minutes of a meeting);
- duplicate documents;
- draft documents and working materials that are used to create a master record or that do not document policy changes or changes in decisions;
- personal messages and announcements; e-mail messages that do not document recommendations, decisions or transactions by public bodies; and
- voice-mail messages

Rough copies of case notes are not transitory records and must be filed with the formal case notes in the client file.

A systematic process for disposing of records by shredding or deleting as information becomes inactive and is no longer needed for business purposes or the long-term operations of the organization will be used.

Records containing personal information will be destroyed by shredding and will not be destroyed by garbage disposal or recycling. These records will not be stored in an unsecured location until destruction, and timely destruction is encouraged.

At a minimum, computer hard drives need to be professionally wiped clean of data before they are disposed of or sold.

Destruction of all non-transitory records will require approval of the Board of Directors with the recommendation of the Privacy Officer and/or the C.E.O.. A record of the destruction of the record will be kept for documentation purposes.

The BGCF will not alter or destroy records to evade a FOIP request, which could lead to penalties or sanctions.

Non-compliance:

Any noncompliance with this policy may result in the implementation of the Progressive Corrective Discipline policy.