bgc Wetaskiwin	**POLICY** Governance	Number B5

Policy Name: Privacy, Confidentiality and Records Management

Policy Statement:
BGC Wetaskiwin will protect the privacy and maintain the confidentiality of its' staff, participants, donors, volunteers, and stakeholders in compliance with Provincial & Federal Legislation and with BGC Canada standards, and will ensure the secure collection, storage, retrieval, and disposal of all records.

Guiding Principles:
Every individual is a valued part of the organization whose unique strengths, interest and personalities are acknowledged, respected and appreciated by all. All individuals are treated fairly, and their personal safety is a priority.

All staff and volunteers model honesty, fairness, positive attitudes, professional ethics, cooperation and respect for self and others. We treat each other as valued colleagues and are mindful in our actions and words. We encourage life-long learning and professional development. All staff and volunteers adhere to the organization's policies, accreditation/licensing standards and all provincial/federal laws that govern our society.

CROSS REFERENCES:
FOIP Act, Information Request Form, Confidentiality Agreement, Release of Confidential Information, Reference Permission Form, Consent Policy, Accreditation Standards, Licensing Regulations, Progressive Corrective Discipline Policy

Original Date	Revision Date	BOARD Approval
October 2005	May 2021	November 2017

Procedure:

Definitions

a) PERSONAL INFORMATION: Any information that can be used to distinguish, identify or contact a specific individual. This information can include an individual's opinions or 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

b) 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 1(q)).

c) 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 participant's file.

1. Collection of Personal Information
    a. The organization will collect information for human resources, program operations and activities of the organization and for no other purposes.
        i. Any collection of personal information will be used for the purpose of offering services, maintaining accountability, program purposes, supervision, and continuity of services.
    b. The individual and/or their legal guardian will consent to information collected.
    c. Documentation must:
        i. Be factual.
        ii. Be objective, reflecting a high degree of professional judgement.
        iii. Avoid unrelated, non-relevant information.
        iv. In most circumstances do not include personal comments and opinions (must be documented as opinion).
        v. Collect any information necessary to provide appropriate services,
        vi. State participant opinions if different from the staff.

vii. Be kept for at least one year after using it. This time period may be decreased if both the organization and the individual mutually agree. The decision to destroy records must be approved by the Program Director and Executive Director.
viii. Identify dates and persons as clearly as possible.
ix. Include only information that is necessary to provide services to the participant.
x. Avoid duplicate material on record.

2. Use of Personal Information:
    a. Staff:
        i. Staff information can only be used for the purposes it was collected for.
        ii. The organization can give reference information to a prospective employer only if the staff provides the previous employment information and the organization may only disclose factual information that represents the staff's job performance.
    b. Participants:
        i. Personal information is to be used only for purposes such as continuity of care, supervision, and case planning. Staff must obtain appropriate consents for any new purposes, such as information sharing.
            1. Written consent shall be obtained from the participant (or legal guardian) before any communication or information is released to any other organization or individual not employed by the organization. If participants request that information be shared they must complete a Release of Confidential Information Form. This form must specify the following information:
                a. With whom the information will be shared.
                b. For what purpose.
                c. For how long the consent will remain in effect.
                d. The form must also include a signature and date of signature.
                e. Staff signature and date of signature.
        ii. Participant information or communications may be shared within the organization only with staff involved with a particular participant and only for the purpose of service delivery. Appropriate staff members may review the participant's file or share information with other BGC Wetaskiwin programs for the purposes of continuity of service and case management.

1. Participant information to be contained or released shall be directly related to delivery of services, determination of needs, or a mutually defined purpose as agreed upon by the participant (or guardian) and staff.

iii. Electronic devices that contain participant information will be passcode protected and any databased containing participant information will be password protected. Passwords cannot be auto-saved.

iv. Electronic participant information will only be sent via facsimile, text, or email to relevant and involved parties.
    1. Any errors in transmission will be protected by a disclaimer, stating "This message is intended for the use of the individual or entity to which it is addressed and may contain information that is confidential and privileged and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please contact the sender immediately and delete if from your system."
    2. All errors in transmission will be reported to the participant and to the Program Director.

v. Staff will preserve confidentiality with respect to any identifying information of any person. When delivering services do not include other participants, friends, or family members without the consent of the participant and/or guardian/caseworker.
    1. If there are other individuals present, they must have a direct relationship to the participant achieving their goal(s).

vi. Staff will testify in court in regards to participant information only if they are subpoenaed.

vii. Participant information or records may be released when:
    1. They are subpoenaed.
    2. Information is disclosed which indicates a risk for suicide and/or threats to harm a person or a child is in need of protection.
    3. The program's contract requires that verbal and/or written reports be submitted.

viii. Contacting emergency services for the safety of staff or participants will not constitute a breach of confidentiality.

ix. If the Privacy Commissioner request information, a release of information is not needed, and the organization must comply with the request.

3. Information Requests:
    a. There are three (3) types of requests: personal, general, and corrections.
        i. Personal Requests are those involving personal information about an identifiable individual.
            1. All participants, legal guardians, staff, and volunteers have the right to access their personal information/records in accordance with FOIP.
                a. Written consent shall be obtained for inactive files/participants (or legal guardian) before any communication and information is released. The applicant must provide enough detail in order to identify the record.
                b. If there are multiple participants 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, them the participant may see portions of their file, which do not refer to other participants. Information relayed by third parties may be blocked.
                c. Staff and 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.
                d. If there are informal files on staff that are separate from personnel files, employees also have access to all information contained in this file.
                e. The organization will make every reasonable effort to respond to a request no later than thirty (30) days after receiving it.
                f. 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.
                g. The applicant may ask to view the record or ask for a copy of the record. The applicant may be charged a fee for copies.

h. An applicant may request the Information and Policy Commissioner to review any decision made by the organization that relates to a request.
i. If the request is for the records of a deceased person, the applicant must be named as the Executor of the Will or appointed as the administrator of the estate by the court. The person must also provide proof of death.

2. If there is involvement with Child and Family Services, Caseworkers and Casework Supervisors will have access to participant files and information with the consent of participants.
    a. Requests for access to records by participants made to a Caseworker will be passed on to the Executive Director who will then block information relating to third parties in accordance with FOIP. If the process is complex, the file may be passed on to the Privacy Commissioner to process the access request.
3. If the Privacy Commissioner requests records, the Executive Director 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 physician).
    a. The organization may make copies of the quested record if records are submitted to the Privacy Commissioner and it is anticipated that the information may be needed.
4. Job applicants can see all 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.
    a. Applicants may request to view any notes that were made by interviewers.

ii. General Requests are those relating to activities of the organization. Examples include requests for a departmental survey, salary scales, job descriptions, and financial reports.
    1. All general requests will be considered upon written request.
    2. All requests must be specific as to correctly identify the record.

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

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

1. 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.
2. Corrections and correction notices will be completed within five (5) business days of the correction request. Exceptions to the correction request include professional opinions and must not be corrected.
3. If the Executive Director refuses a correction request, the information in question will be linked to the correction request for future reference.
4. Notification of other parities 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.
5. If the person requesting the correction is unsatisfied with the correction or decision of the Executive Director to not complete a correction, the individual may contact the Privacy Commissioner.

4. Records Management
   a. The organization will maintain a records system, which may be computerized or manual, which captures, maintains, and provides access to records over time.
      i. 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.
   b. The organization will create records only to operate its program and services and will not produce information that is not required.
   c. The organization will maintain a records system in order to identify, locate and produce records in response to information requests.
      i. This system may be maintained by individual programs.
         1. All files are archived to the file storage rooms, located downtown and at the Robert B. Colborne Centre for the life of the organization.
   d. All records will be stored in a secure location, which will not be accessible to individuals other than staff. If staff are required to transport or take participant

information out of the building, they are required to protect and secure it and return it to the participant file as soon as possible.

e. Some recorded information can be managed as a transitory record which has a short-term value and may be disposed of regularly at the discretion of an employee:
    i. Information of short-term value (e.g. notes kept to prepare official minutes of a meeting).
    ii. Duplicate documents.
    iii. Draft documents and working materials that are used to create a master record or that do not document policy changes or changes in decisions.
    iv. Personal messages and announcements.
    v. Email messages that do not document recommendations, decisions, or transactions by public bodies; and voice-mail messages.
    vi. Rough copies of case notes are not transitory records and must be filed with the formal case notes in the participant file.
f. 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.
    i. The following types of records may be destroyed as follows:
        1. After seven (7) years
            a. Financial Records
            b. Donor Records
            c. Contracts and Agreements
        2. After one hundred (100) years
            a. Participant registration and consents forms
            b. Participant Files
            c. Case Notes and individual participant reports
            d. Critical Incident Reports, including Abuse Reports
            e. Personnel Files
            f. Agreements with Staff and Board Members
            g. Communication Logs
            h. Board Meeting Minutes
            i. Volunteer Files
            j. Annual Reports
            k. Insurance Policies
    ii. Records containing personal information will be destroyed by shredding and will not be destroyed by garbage disposal or recycling.
    iii. These records will be stored in a secure location.

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

g. Destruction of all non-transitory records will require approval of the Board of Directors with the recommendation of the Executive Director.
   i. A record of the destruction of the record will be kept for documentation purposes.

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

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