BCRGPL- 015: Confidentiality and Privacy

Applies to: Management Committee, Executive Officer, Employees, Stakeholders and Service Users
Specific responsibility: Management Committee, Executive Officer, Team Leaders

POLICY STATEMENT

BCRG upholds the rights of service users, carers and families to privacy and confidentiality of information regarding background, health status and other personal information and takes steps to ensure that privacy is maintained under all reasonable circumstances.

BCRG recognises that service users, carers and families have the right to access information about themselves, held by the service.

BCRG conforms to both state and commonwealth privacy legislation requirements regarding the collection, use and protection of personal information of our service users and employees/volunteers.

PURPOSE

The purpose of BCRG Confidentiality and Privacy policy and procedures is to provide a framework to collect, use, store, secure and disclose personal information, sensitive information and health information provided to the organisation by clients, visitors, individuals, employees, stakeholders in accordance with the Australian Privacy Principles (APP) and the Federal Privacy Act 1988, and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

POLICY PROTOCOLS

Confidentiality refers to the obligation of non-disclosure by this agency of personal information unless it has the consent of the person concerned.

BCRG will ensure privacy and confidentiality by:

- Collecting only the information required for service delivery;
- Informing people of the purpose for collecting the information;
- Providing individuals with access to their information held by the service;
- Disclosing personal information to 3rd parties only with the written consent of the individual;
- Securely storing service users personal information; and
- Destroying information in accordance with the Archives Act 1983.

BCRG has an obligation to report personal information where there is:-

- Disclosure of a crime or intended crime;
- Where the person is suicidal, his/her safety is at risk of personal harm or being abused by another; and
- To warn a third party who is in danger.

BCRG adheres to the Australian Privacy Principles in accordance with the Australian Privacy Principles (APP) and the *Federal Privacy Act 1988*, and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*

BCRG will only transfer personal information about a service user or employee/volunteer to someone who is in a foreign country if it is believed that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles

AUSTRALIAN PRIVACY PRINCIPLES 2014 - Summary

APP 1 — Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.
APP 4 — Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

The Australian Privacy Principles guidelines and Read the Australian Privacy Principles can be obtained by the following link:
https://www.oaic.gov.au/privacy/australian-privacy-principles

DEFINITIONS
Personal information –refers to information that provides information or an opinion (including database information), whether true or not, recorded in material form about an individual whose identity is apparent or can reasonably be ascertained from information or opinion.

Sensitive information covers the information or an opinion about an individual's:

- Race or ethnicity, sexuality and/or sexual preferences & practices, membership to groups, organisations, political and professional associations or trade unions, child protection issues, personal/family interactions, criminal record, political preferences, philosophical beliefs, religious beliefs or affiliations, health information and generic information about an individual that is not otherwise health information.

Health information covers personal information or an opinion about an individual that includes:

- Health or disability (physical, mental or psychological health at any time), an individual's personal preferences for medical treatment, service provision or restrictions in health care, general information provided in relation to health care, health services and treatment, personal preferences in relation decisions about the individual's body organs such as donations for kidneys, body substances, or body parts, other personal information about genetic information about the individual which could be predictive of the health (at any time) of the individual.

Employee records:

- Relates to information obtained and stored in relation to employment of the employee. This also covers details collected and stored about Board members.

While the organisation acknowledges the information relates to individuals, it will also treat all information it receives from meetings, organisations, visitors, suppliers and other stakeholders in a private and confidential manner similar to individual's information.

PROCEDURES
BCRG is committed to ensuring that details about service users, employees and volunteers are kept confidential and only disclosed with the persons' permission. This procedure is aligned to the Principles of the Privacy Act. The purpose of this procedure is to give information regarding the various aspects of service delivery where privacy & confidentiality are essential. Specific procedures regarding each topic are detailed in other parts of this Policy & Procedure manual. The Executive Officer will review all funding agreements to ensure that the organisation's privacy procedures remain compliant with all funding requirements.

The following aspects of service provision are considered to require consideration of confidentiality and privacy:

Storage of Information/Client Files
Information about individual clients is stored in the following ways: -

- Hard copy
- Electronic database

Hard copy files are stored in locked filing cabinets within BCRG offices

Disposal of documents
BCRG uses a document disposal system for the destruction of records containing personal information that is no longer required. Archived material – material no longer used by BCRG – after having been held for 12 months following closure of the file, (is archived in hard copy or electronically for 7 years before secure destruction). In the case of children, identifying information and records of incidents and accidents are stored until the child is 25 years of age.
After these periods, client files are disposed of by shredding or removal by a contractor specialising in secure destruction of documents.

Collection & Provision of Information

- The only information held by BCRG about a service user will be information necessary to assess the need for a service and to provide the service. Information should be non-obtrusive and objective as possible, yet relevant and up to date.
- The only information held by BCRG regarding employees/volunteers will be personal information required for the employment/recruitment of employees/volunteers.
- All entries in service user and employee/volunteer records will indicate the time and date when the entry was made and enable the reader to identify the name and designation of the writer.
- All service user and employee/volunteer note entries will be either written in ink so that they will not fade or be erased.
- BCRG will provide service users and employees/volunteers information regarding the purpose and use of personal information including who will have access to this information.
- Service users and employees/volunteers will be informed of their right to withhold information or provide information anonymously, if applicable.
- Service users and employees/volunteers will be informed of how to make a complaint regarding the collection, storage or use of their personal information.

Responsibilities for managing privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- Senior management and team leaders are responsible for content in BCRG publications, communications and website, and must ensure the following: -
  - Appropriate consent is obtained for the inclusion of any personal information or photographs of any individual including BCRG personnel.
  - Information that is provided by other organisations or external individuals conforms to privacy principles
  - That the web site displays a Privacy statement that clearly identifies the conditions of any collection of personal information from the public via their visit to the web site.
- The Executive Officer and Administration Officer are responsible for safeguarding personal information relating to BCRG staff, Management Committee members, volunteers, contractors and BCRG members.

Access to and Disclosure of Information

- The consent of the service user or employees/volunteers must be obtained to utilise the service user's/employees/volunteers name, photographs, videos or voice that identify an individual
- The Executive Officer and Management Committee members are the only people authorised to divulge information related to employees/volunteers, where it is legally and ethically justified.
- Only employees/volunteers with a need (i.e. those involved with the care or support of a service user, supervision of employees/volunteers) will have access to personal information related to service users or employees/volunteers.
- Service users and employees/volunteers will be made aware of their right to access their personal records by appointment and to request a copy of any document contained therein. When this is requested, it will be done in the presence of the Executive Officer. This right will also be made clear in employees/volunteers handbooks and service user information packs.
- Access to employee records is restricted to the Executive Officer, Management Committee Members and/or Administration Officer.
- In cases of emergencies the 'First Contact' or nominated person/advocate on the service user case file/ information sheet will be contacted to make immediate decisions about wellbeing. Where a Duty of Care matter arises after reasonable discussions have concluded that a decision must be made 'First Contact' will provide permission.
- Service users have the right to access any personal information kept about them by the service. Requests from service users to access files should be referred in writing to the Executive Officer who should ensure that assistance is provided for the service user to access information on his/her file within two weeks. An employee/volunteer should be made available to explain any terminology to the service user.
- When a service user joins the service they are advised of the privacy and release of information procedures within the organisation including that information is kept confidential and is kept in locked filing cabinets or on a computer that only appropriate employees/volunteers have access to.
- Information that is passed on is marked 'private and confidential' and the computer protected with security firewalls.
- Personal information will only be faxed or emailed if the receiving agency can ensure the security of the information provided.
- The only people authorised to read a service users' file are the service user themselves, the service users' carer, the service users' advocate and the service users' legal guardian. Carers of adult service users and advocates must have the service users' permission, where this can be given.
- Access to some information may breach confidentiality of employees/volunteers or another service user and this information may be withheld.
- Consent to Release Information Form is to be used when information is being released for any other purpose than referral.
- Personal information regarding a service user or employees/volunteers may be disclosed if:
    - Informed consent is obtained from the person and this consent specifies the precise information and purpose for the disclosure;
    - There is a serious and imminent threat to an individual's life, health or safety;

- There is a serious threat to public health or public safety; or
- There is a legal obligation under the Crimes Act 1900 (NSW), the Crimes Act 1914, or the Coroners Act 1980 (NSW) to notify police about serious criminal offences, or the coroner's office regarding investigations involving the death of a person.

- Confidentially is between the service user and BCRG (not particular employees/volunteers) Employees/volunteers will inform the service users if they have to report any information that may impact upon the service provided to the office.

Where a service user requests to access their file the service user and the Executive Officer agree on a mutually suitable time and the following occurs:

- A quiet, private area is offered to the service user/stakeholder
- A team leader or employee remains in the room with the service user at all times when information is being accessed
- Requests for support from an advocate/friend are accepted
- The person seeking access may take notes of the information, but copies cannot be provided to a third party
- Should the service user query the accuracy of the information in the file, the service requests supporting evidence prior to adjusting the file
- Should the service user object to information in the file they are invited to make a formal complaint.

The Executive Officer, team leaders and employees respond positively to requests from service users/stakeholders to access their personal information according to the requirements of the Freedom of Information Act 1989 (NSW).

Steps	Action/Evidence	Who does it	When
1	Service User indicates their wish for information to be released	Service User	Anytime
2	Release of Information Form is completed	Service User	Anytime
3	Information is released	Executive Officer	After consent obtained
4	Consent to release information filed in Service Users file	Executive Officer	After information released

Storage of Personal Information

- Service Users or Employees/volunteers will be informed of the Service' responsibilities in relation to the protection of personal information through:
  - Service User Information Packs;
  - Service Agreements; and
  - BCRG policies regarding privacy and confidentiality.
- All computers containing information regarding service users and employees/volunteers will be password protected. Passwords will be recorded on the Computer Password Register which will be kept in a secure location by the Executive Officer of BCRG
- Any Sub Contractors which the service utilises will be required to provide confirmation that their policies and procedures comply with the appropriate privacy laws.

- The anonymity of service users and employees/volunteers will be preserved for purposes of research, case presentations or conference papers.
- Personal information should only be copied when it is essential to do so.
- Service user files and employees/volunteers files will be filed separately to generalist service administration files. Service user files and employees/volunteers files will be kept locked when not in use. Keys to service user files and employees/volunteers files will only be provided to personnel with authorisation to access these files.
- Files removes from the office should be placed inside a plain manila folder which does not identify the service users and employees/volunteers.

Steps	Action/Evidence	Who does it	When
1	All Information kept on computer is password protected	All Employees/volunteers	Ongoing
2	Filing Cabinets containing Service User/Employees/volunteers files are kept locked with limited authorised access.	Authorised Employees/volunteers Only	Ongoing
3	Each Service User will have a separate file created in hard copy and on computer	Assessor	At point of Assessment
4	Each Employee/volunteer will have a separate file created in hard copy and on computer	Management	At point of Employment or recruitment

Length of time records are held

If a Service User ceases to access BCRG but may need to resume service at a later date, information relating to the Service User will be kept for a period of 2 years before being archived. If the service will definitely not be resuming, Service User's records will be archived at the end of the financial year. All information regarding Service Users will be shredded seven (7) years after they cease to receive services.