Privacy Policy

Version 01.00 dated 19/03/2019

PURPOSE

The purpose of this Policy is to clarify Youthrive's decisions and position relating to privacy practices within the organisation. Youthrive is bound by the Privacy Act 1988 (Cth).

SCOPE

This Privacy Policy sets out how Youthrive complies with its privacy obligations regarding the collection, use, disclosure, storage and security of personal and sensitive information and applies to all Youthrive staff.

POLICY STATEMENT

Youthrive is committed to ensuring information management is consistent with best practice and applicable laws. Mishandled or compromised information has the potential to cause a loss of trust and considerable harm to reputation. Depending on the nature of the breach it may seriously impact on business operations or have detrimental consequences to the individuals concerned.

Youthrive staff share a personal responsibility in protecting client information. Staff are expected to conduct themselves in an ethical and professional manner ensuring information is only collected via lawful and fair means, and managed in accordance with Youthrive policies and procedures and obligations under privacy related legislation.

Types of Information We Collect

Youthrive only collects necessary personal and sensitive information about individuals that will enable us to:

- Provide requested supports and services;
- Carry out our functions and activities;
- Meet our statutory or legal obligations.

The information we collect about individuals varies and is dependent on the circumstances of their engagement with Youthrive.

The Privacy Act 1988 (Cth) provides a definition for information categorised as 'Personal' and 'Sensitive'.

Personal information is defined as: information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Common examples are an individual's name, signature, address, telephone or mobile number, email, date of birth, medical records, bank account or credit card details, photos, video's, case notes and commentary or opinion about a person (e.g. reference checks).

Sensitive information is now defined as a type of personal information which includes:

- an individual's racial or ethnic origin
- health information

- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record

Collection of Solicited Information

Youthrive is permitted to collect **Personal information** about an individual provided the information is reasonably necessary for, or directly related to one or more of our functions or activities. Where it is reasonable and practical to do so, we will only collect personal information about an individual from the individual concerned.

We are further permitted to collect **Sensitive information** about an individual provided:

- the individual consents to the collection of that information and
- the information is reasonably necessary for one or more of our functions or activities; or
    - the collection of information is required or authorised by or under Australia law; or
    - a permitted health or general situation exists; or
    - the information relates to our activities, and the information relates solely to members or individuals who have regular contact with Youthrive in connection to our activities.

Youthrive has a Privacy Statement. This Statement ensures individuals are informed of the reasons why we require their information, the types of information we collect and how we will use it, their privacy rights, complaint mechanisms and how we will manage their information and protect their privacy.

Unsolicited Information

If Youthrive receives information about an individual that we have not requested, staff members are required to make assessment to determine whether or not;

- the information is necessary to our functions or activities; and
- the information would have been provided to us had we requested it.

If the information is not relevant to our functions or activities, or we would not have been able to obtain it via lawful and fair means; we are required by law to destroy or de-identify the information as soon as practicable provided the information is not contained within a Commonwealth record and it is lawful and reasonable to do so.

Use and Disclosure

Relevant to the primary purpose under which an individual's information is collected; Youthrive typically uses and/or discloses information about individuals in a manner that enables us to:

- Identify individuals
- Recruit and employ staff
- Recruit and engage students
- Work collaboratively with other stakeholders
- Provide requested supports and services
- Conduct permitted marketing activities
- Meet our statutory and legal obligations
- Report internally
- Conduct research and program evaluations

Youthrive will not use an individual's information for any secondary purpose nor disclose their information to any third party without first obtaining their consent. As an exception to the rule, Youthrive is permitted to use or disclose an individual's information for a secondary purpose provided that:

- Obtaining the individuals consent is unreasonable or impracticable;
- The individual concerned would reasonably expect us to use their information for that purpose;
- The secondary purpose is directly related to the primary purpose under which their information was collected.

Exemptions

Youthrive is exempt from rulings pertaining to the collection, use or disclosure of an individual's information (both personal and sensitive) when:

1. It is required or authorised by or under an Australian law or a court/tribunal order; or
2. A permitted general situation exists; or
3. A permitted health situation exists; or
4. We believe the information is necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

A **Permitted General Situation** exists when:

- It is unreasonable or impracticable to obtain the individuals consent and we reasonably believe that the collection, use or disclosure of is necessary to lessen or prevent a serious threat to the life, health (physical or mental health and safety) or safety of any individual or to public health or safety.
- We believe the collection, use or disclosure will assist in locating a person who has been reported as missing.
- We suspect that unlawful, or misconduct of a serious nature that relates to our functions or activities has been, is being, or may be engaged in and we reasonably believe that the collection, use or disclosure is necessary in order to take appropriate action.
- The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
- The collection, use or disclosure is reasonably necessary for a confidential alternative dispute resolution process.

A **Permitted Health Situation** exists when:

- The collection of health information is necessary to provide a health service to the individual and either:
    - The collection is required or authorised by or under Australian law, or
    - The information is collected in accordance with the rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind Youthrive
- Additional health situations apply for the purposes of conducting research, compiling or analysing statistics, management, funding or monitoring of a health service. Please refer to 16B of the Privacy Act.

On each occasion when an individual's information is collected, used or disclosed in accordance with one or more of the above exemptions; we are required by law to record the circumstances related to the event. Please refer to the Privacy Act 1988 (Cth) or Information Privacy Act 2009 (Qld) for further information pertaining to privacy exemptions.

Consent from Youthrive adult clients

Unless required, permitted or exempt by law, Youthrive will not collect, use or disclose personal or sensitive information about a client without first obtaining their written consent.

Where permitted by consent; information will be gathered directly from the client concerned in addition to the nominated third parties the client believes is important in providing them with ongoing supports and services and/or will enable Youthrive to better assist them and their family.

Prior to engaging our services, staff must ensure clients have a thorough understanding of:

- the services provided by Youthrive;
- the Client Privacy Statement; and
- what is being acknowledged and agreed to by signing the Consent Form.

Throughout their engagement with Youthrive, clients must be kept informed about the types of information we collect about them and their family, and how it will be used.

Consent from Youthrive child and young person clients

Although privacy legislation does not stipulate an age when a child or young person can make decisions about their own personal information, there are precedents that support the capacity of young people to make decisions about their own personal information.

For young people who understand the concept of privacy, Youthrive staff should read them the Client Consent form and ask them to sign it. In cases where Youthrive staff believe a child or young person has the capacity to understand the concepts implied, in best practice, staff should consider seeking their consent.

When seeking informed consent from a child or young person, the consent process should be explained in simple language that is developmentally appropriate to ensure understanding. It is important to that they understand why we need their consent, what they are consenting to and implications associated with providing consent.

Informed consent may also be verbally obtained from the child or young person while in the presence of their parent/s or guardian/s.

Written consent must also be obtained from the child or young person's parent/s or guardian/s using the Client Consent form.

Obtaining consent for those unable to provide consent

Where the individual is physically, mentally or legally incapable of providing/communicating consent; consent can be obtained from a parent, spouse or de facto, family member, caregiver, guardian or legal representative. Please refer to the Privacy Act 1988 (Cth) and Information Privacy Act 2009 (Qld) for further information and definitions of whom is recognised as a family member, care giver or other representative acting on behalf of an individual.

Reporting

To protect the privacy of individuals, information used for internal reporting, research and program evaluations must be de-identified prior to use or disclosure. This means ensuring the information used or disclosed does not contain information that could identify, or is likely to identify an individual or their family.

Identifiers

An identifier is defined by the Privacy Act 1988 (Cth) as a number, letter or symbol, or a combination of

any or all of those things, that is used to identify an individual or to verify the identity of an individual.

Some relevant examples include:

- The NDIS number or HCWA Client ID
- Child Safety Blue Card, Drivers Licence or Medicare Card registration number
- Tax File Number
- Superannuation Membership Number

Youthrive will not adopt, use or disclose a government or other organisation related identifier of an individual as its own client identifier.

Information Integrity

All staff have a personal responsibility of ensuring that the information we collect, use or disclose is accurate, up to date, complete and relevant to the purpose of the use or disclosure.

With the nature of our functions and activities; data integrity is a fundamental and critical factor to ensuring Youthrive remains operational and compliant with our statutory and legal obligations.

For example, the information recorded about individuals may be used to:

- Comply with a judicial proceeding, court order or legal process
- Provide appropriate and ongoing supports and services to individuals
- Generate statistics and reports to meet our statutory and legal obligations
- Support funding requests and/or variation requests
- Validate workforce needs, development and growth
- Validate service requirements within our regions
- Evaluate the effectiveness of our programs and services
- Perform in house training using case studies/client records
- Conduct research

Staff can ensure the reliability of the information they manage by following information management procedures and practices implemented within their team, participating in training opportunities to develop or maintain competency in using information management systems and promptly correcting or notifying others of any noted discrepancies within existing records.

Team Leaders/Clinic Coordinators are responsible for overseeing the integrity of data captured within their team. Team Leaders are to ensure staff are appropriately trained prior to accessing information management systems and records, and to further ensure the reliability of recorded data through auditing and monitoring.

Access to Information

Individuals have the right to request access to their own information held by Youthrive. When an individual enquires about accessing their information, staff will inform them of our decision making process and response timeframe (refer below), and seek their request in writing specifying what information they want access to.

Prior to permitting or declining a request; staff will make an assessment based on the individual's circumstances and the following permitted exemptions under which we can decline (please refer to privacy legislation for further and more detailed information pertaining to privacy exemptions):

- we believe granting access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- we believe granting access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;

- the information relates to existing or anticipated legal proceedings between Youthrive and the individual;
- providing access to the information may prejudice Youthrive' negotiations with the individual;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order;
- providing access would prejudice an investigation of possible unlawful activity;
- providing access would be prejudicial to the physical or mental health of that person;
- providing access is contrary to the individuals best interests - unable to understand the information and context in which it was recorded and are unable to make judgement as to what might be in his or her best interests

Where it is likely that a request will be permitted, prior to providing notification of the outcome or allowing access; the individual's requested information must be thoroughly reviewed by clinicians involved with the client and the relevant Team Leader/Clinic Coordinator to ensure that if there is information recorded about another person, we:

- Obtain written consent from the person to disclose their information; and/or
- Redact all or requested information pertaining to the other person to protect their privacy

When access is permitted

Individuals will be notified within ten (10) working days of the outcome of their request from when the request was made.

With consideration to the nature of the information requested and our obligations to protect the privacy of individuals, Youthrive will enable individuals to access their information in a setting and/or manner that is reasonable in the circumstances and will employ appropriate measures to verify the identity of the individual prior to granting access.

As a preference, clients will be requested to visit a nominated Youthrive office to access their information. Accompanied by a suitably qualified staff member, clients will be given use of a private space within the Youthrive office to view and/or discuss their information.

If the client is unable to visit a Youthrive office; staff must consider alternative mutually agreeable arrangements (as are reasonable in the circumstances) to enable access. Given the nature of the information we collect from clients, providing information via registered post or email should be considered as a last resort.

When access is declined

Prior to declining access; as part of the decision-making process, staff must consider mutually agreeable solutions (as are reasonable in the circumstances) to provide sufficient access in a way that will meet the needs of the individual and Youthrive. If a mutually agreeable outcome cannot be found; staff will notify the individual in writing within ten (10) working days from when the request was made.

The letter must outline;

- the reasons or grounds for the refusal (where reasonable to do so); and the section of the Privacy Act 1988 (Cth) under which we refuse access; and
- mechanisms available to the individual to complain about the refusal; and
- any other matter prescribed by the regulations.

Correction of Information

Youthrive is required to take reasonable steps to ensure the information we hold about individuals is

accurate, up to date, complete, relevant and not misleading. If practical, lawful and requested by the client, Youthrive is required to notify the entities we previously disclosed the individual's information to about any corrections we have since made to that information.

If an individual believes that the information Youthrive holds about them is inaccurate, incomplete or not up-to-date they have the right to request that we correct their information. Upon enquiry, staff will inform them of our decision-making process and response timeframe, and seek their request in writing specifying what information they believe is incorrect and the proposed correction/s.

Youthrive is permitted to refuse the request if we disagree with the individual about the accuracy, completeness and currency of their information. If we decline the request, individuals will be notified of our refusal via letter which must outline;

- the reasons for the refusal (where reasonable to do so); and
- the section of the Privacy Act 1988 (Cth) under which we have the right to refuse; and
- mechanisms available to the individual to complain about the refusal; and
- any other matter prescribed by the regulations.

The individual's written statement and/or a notation must be attached to their Youthrive record, and must specify which aspects of the information is considered to be inaccurate, out-of-date, incomplete, irrelevant or misleading by the individual. The statement/notation associated with the individual's record must be attached in such a way that it is apparent to all users of the information.

Anonymity and Pseudonymity

Where lawful and practical; individuals must have the option of not identifying themselves, or of using a pseudonym when dealing with Youthrive in relation to a particular matter.

Youthrive's position is that when an individual contacts us for general information or to lodge a complaint, we respect their right to exercise anonymity by not providing us with their personal details.

Information Security

Mishandled information can cause a loss of trust and considerable harm to our reputation: additionally, if information is lost or altered without authorisation, it can have a serious impact on our capacity to perform our functions or activities. Youthrive has security obligations under The Privacy Act 1988 (Cth) to take reasonable steps to protect information from misuse, interference, loss and unauthorised access, modification and disclosure.

We employ a number of measures to minimise security risks and prevent a breach of privacy and security. The below points briefly outline the core areas including, but not limited to:

- Staff are expected to conduct themselves in a professional and ethical manner in accordance with the Youthrive Code of Conduct Policy and Confidentiality Statement and where applicable, relevant health or medical professional confidentiality and record keeping obligations.

- Physical and electronic information is stored and accessed in a controlled and secure manner in accordance with the Records Management Policy and other relevant policies and procedures

- Information is collected, used and disclosed in accordance with this Privacy Policy, the Privacy Act 1988 (Cth) and other relevant Acts and legislation.

- The security, retention and destruction of information is managed in accordance with the Youthrive Records Management Policy, Privacy Act 1988 (Cth) and health or medical professional record obligations.

Direct Marketing

Youthrive is permitted to use or disclose personal information about an individual for direct marketing who is a client of an Youthrive service providing:

- we collected the information from the individual about whom it relates;
- the individual would reasonably expect that their personal information would be used or disclosed for direct marketing purposes;
- we provide a simple means by which the individual can request not to receive direct marketing; and
- the individual has not already made it known that they do not consent to being contacted for direct marketing purposes.

Where an individual is not a client of a Youthrive service and would not expect Youthrive to use their personal information for direct marketing, or where we have collected their information from a third party, we are only permitted to use or disclose their personal information for the purpose of direct marketing providing;

- the individual has consented ;
- we provide a simple means by which the individual can opt out of direct; and
- each direct marketing communication sent by Youthrive includes a prominent statement telling the individual that he or she may request to no longer receive direct marketing, and no request is made.

The use or disclosure of sensitive information for the purpose of direct marketing is only permitted when written consent has been provided by the individual.

Privacy Complaints

Complainants should be informed of the Youthrive complaints process and the Client and Stakeholder Complaint and Feedback Policy and Procedure.

All complaints must be recorded and managed according to the appropriate complaint category i.e. a breach of privacy/confidentiality complaint is a Category 3 complaint – refer to the Youthrive Client and Stakeholder Complaint and Feedback Policy and Procedure for direction.

POLICIES, PROCEDURES, RECORDS & FORMS

- *Privacy Statement*
- *Consent Form*
- *Records Management Policy*
- *Code of Conduct*
- *Confidentiality Statement*

LEGISLATION, STANDARDS AND GOVERNING BODIES

- *Privacy Act 1988 (Cth)*
- *Privacy Amendment (Notifiable Data Breach) Act 2017(Cth)*
- *Information Privacy Act 2009 (QLD)*

MODIFICATION HISTORY

Document Owner:		Document Approver:	Date to be reviewed:
Youthrive		COO	March 2020
Date	**Version**	**Modification**	
05/01/2015	V0.01	Creation of policy	
19/03/2019	V2.0	Reformatted & re-issued from previous document titled Privacy Policy V0.01, to be in line with Act for Kids Privacy Policy	