Privacy and Confidentiality Policy

Policy Number:	***QYS-DSER 4.1***
Approved by Board on	***19 Nov 2014***
Reviewed On:	***April 2017***
	October 2020

Introduction

The *Australian Privacy Principles* (APPs) are a single set of principles that apply to agencies and organisations. Queensland Youth Services (QYS) has applied these principles in formulating the organisation's *Privacy and Confidentiality Policy*.

A person has the right to:

(a) Not have their personal privacy, family home or correspondence unlawfully or arbitrarily interfered with; and
(b) Not have their personal reputation unlawfully attacked.

Section 25 – Human Rights Act 2019.

Purpose

The purpose of this document is to provide a framework for QYS in dealing with confidentiality considerations and to ensure adherence to the *Information Privacy Act 2009*, the APP principles, and the *Human Rights Act 2019*.

Policy

QYS collects and administers a range of information for a variety of purposes. The majority of this information is restricted in its circulation for commercial, privacy, or ethical reasons.

Collection of personal information will be lawful, fair, reasonable and unobtrusive.

All Management Committee (MC) members, employees, volunteers and students must accept QYS *Privacy and Confidentiality Policy QYS-DSER4.1* on QYS' Human Resource Management System (*Happy HR)* before commencing duties or placements.

Breaches of confidentiality will result in disciplinary procedures, including potential dismissal or legal action.

Confidentiality may be breached when it is considered to prevent harm to an individual or the public, or when the 'duty to warn' principle applies.

Clients (a young person supported by QYS) are informed of what information is collected, and the purpose for collecting information.

QYS employees will outline to the client the circumstances in which their personal information may be used or disclosed to another agencies or organisations.

QYS may disclose personal information if it is deemed necessary to prevent serious threats to the health and safety of the client. There may be circumstances were QYS is legally required to disclose information.

Sensitive information must be filed in lockable storage, which is only accessed by, or disclosed to, employees who need the information to fulfil their responsibilities or have a legal right for access. Client information stored on a computer must require a password for access.

When client information is no longer required, it is to be destroyed by shredding or incineration. Note archived records are kept for 7 years before being shredded or incinerated. Refer to QYS' *Document Retention and Destruction Policy QYS-GOV2.10*.

QYS employees will take reasonable steps to ensure that information collected is accurate, up to date, complete and relevant to service requirements.

An employee/client may request in writing to the CEO to see what personal information is being collected about them under the *Information Privacy Act 2009*. Access must be given within 30 days in a manner that is reasonable and practicable. Reasons for any refusal to provide access must be provided in writing.

Employees must respect all dimensions of a client's privacy:
- privacy of the body
- privacy of the home
- cultural issues

When sensitive matters are being discussed with the employee, appropriate physical space arrangements should be made available to the client.

Types of information collected by QYS:

Employees
- personal details (name, D.O.B., address, phone numbers, resumes, Blue Card, driver's licence, qualifications etc.)
- bank account details, Tax File Number
- superannuation fund
- workers compensation claims
- performance management (appraisals etc.)

Clients
- personal details (name, DOB, guardian, address, contact details etc.)
- referral forms, case workers with other agencies/organisations
- case plan/s (collaborative case management)
- case file notes
- medical history
- information from other agencies
- brokerage expenditure (where applicable)

Any breaches to employee/client privacy are to be reported immediately to the CEO, and to the relevant Department in accordance with service agreement provisions.

Client Privacy on digital devices

- Employees are not to access a client's digital device (phone, tablet, computer etc.) without the client's direct consent and presence. The consent should be specific about what access is being approved, e.g. access to photos, contacts, apps

- The client must be informed of the purpose of accessing device, and consent to how any information on the device is actioned.

Confidentiality in the workplace

All matters discussed at staff meetings, committee meetings and during the day-to-day operations of the service will be treated as confidential. All QYS files, accounting documents, procedures and any information gained through service operations is considered confidential.

Employees will protect the privacy and confidentiality of other employees by not providing personal information about them to anyone either within or outside the service.

Employees and those placing applications for employment with QYS will have their personal information treated with privacy and confidentiality. The procedure for storing and disposing of employee and prospective employees' personal information is the same as granted for clients.

Information about employees may only be accessed by the CEO and the employee concerned. Employees wishing to access their file may do so under supervision of the CEO.

Resources

Australian Privacy Principles (July 2014)

Information Privacy Act 2009

Human Rights Act 2019

QYS' *Document Retention and Destruction Policy QYS-GOV2.10*