Strategic Objective:
1. Excellence In Service Delivery

POLICY :	1.4	Quality		
PROCEDURE:	**1.4.6**	**Confidentiality and Privacy**		
Approval By:		Quality Manager	**Approval Date:**	13-05-2013
Document Owner:		Systems and Risk Manager	**Next Review Date:**	13-05-2017

Purpose

The purpose of this procedure is to ensure that all material of a confidential nature is collected, recorded, maintained and released in a manner that ensures privacy and confidentiality according to legislative requirements.

The Systems and Risk Manager is responsible for establishing, controlling, and maintaining the system for recording, storing, releasing and destroying confidential information.

The Systems and Risk Manager (or delegate) is responsible for the sensitive collection, recording, and storage of confidential material They must also ensure that clients, carers and guardians understand the procedure by which they can access their own personal records during an episode of service and after program exit1.

The Chief Executive Officer (or delegate) is responsible for the:
Implementation of appropriate security measures over access to database records, word processing and any other documents on clients.

Ensuring appropriate security mechanisms (passwords, firewalls) are in place before connecting QEC's computers to the Internet or any external network of computers.

Target Audience

All QEC staff, contractors, clients and visitors

Definitions

FOI – Freedom of Information
Visitor – any person attending a QEC site, client or staff member
Client – A person attending a QEC program

Procedure

QEC client records should hold no surprises for individual clients, documentation being compiled by QEC staff in partnership with clients. Clients may access their written records; the only exception to this policy being where it is reasonably believed that revealing an entry to a client will threaten the safety of any person. (See Client Access below).

Collection of Confidential Information

- QEC staff will ensure that they obtain clients' consent to provide essential personal information and will inform clients that their information is retained securely. QEC Privacy brochure is issued to every family beginning a QEC program.

[1] Access to information/records after program exit is available under Freedom of Information legislation. Process is by a written request to the CEO, QEC.

- QEC staff will only collect information that is needed by QEC to perform its role as provider of Early Parenting assessment, care, support and education services, and to monitor service provision. They must not seek more information about the client than is necessary to perform the role of service planner, provider and evaluator.

Recording of Confidential Information

- Staff must record information in an objective, professional manner based on professional judgement. All written material must be free of personal judgements, and must accurately represent the information, event or interaction that is being recorded.
- All staff must appropriately record whether the information is discussed or observed and its source for client files.
- Staff must be aware that clients or authorised agencies may access clients' records at a later stage.
- All staff must write file, and other, notes in a manner that can be readily understood by clients, carers and guardians, service providers and staff.
- For paper records, staff members will enter signature, qualification, date and time for each recorded entry.
- For electronic records, automatic details of login user title and time for each recorded entry will be made by the client information system.

Storing of Confidential Information

Paper Records

- Admitting Staff and Clinical Teams must ensure that all records are stored in a secure manner.
- Records should be securely attached to a client folder or patient history file.
- These files must be stored in a filing cabinet in the Programs office, when the client is receiving QEC services.
- Folders containing client records are stored in the primary storage area in the Administration Wing, or applicable Program office that is locked.
- All relevant areas are locked when staff are not in attendance.
- After three years, folders containing confidential client records are transported and stored in secure secondary storage off site (see Admission and Unit Support Procedure Manual).
- When taken from the office for a home visit or case meeting, files must be transported so that individual files are not visible, or accessible to unauthorised persons.

Electronic Records

- Computer systems containing confidential information must have appropriate security controls to prevent unauthorised access.
- Staff with access to computer systems must ensure that they

keep their access passwords secure.

- System passwords prompt to be changed at regular periods. If not changed, will expire.
- Appropriate security measures are put in place to prevent unauthorised access to files deemed not for viewing by all staff.
- Before connecting to the Internet or external networks of computers, the highest practical level of security should be in place (for example, firewall and password control), and the risk of unauthorised access to confidential material virtually eliminated.

Access to Confidential Information

Staff access

- Confidential information should only be accessed by staff who have a need to access that information to undertake their duties.
- Program Managers will ensure that all staff are aware that access to files in the compactus should only be by staff who have need for the information to undertake their duties. A tracer card must be inserted in place of the removed record clearly showing the UR Number and/or file name, name of person removing the file and date. Access to files in Program offices is only accessible to appropriate QEC staff.

Client access

- Clients may access their own records at any time they are receiving QEC services. If it is reasonably believed that revealing an entry to a client will threaten the safety of any person. The CEO or delegate must be informed and will decide action to be taken.
- Past clients may access their records by following the procedure and making the prescribed payment set down in the Freedom of Information Act and Regulations. Requests in writing received from past clients are managed by the CEO or delegate.

Access by another agency/organisation

- Confidential Information will generally only be released to persons with consent from the client.
- If requests for information come from external parties not authorised by the client, such requests will be referred to the CEO or delegate who will assess whether it is necessary to seek the permission of the client. The CEO or delegate can decide whether there is an overriding responsibility from duty of care, to release confidential information.
- Requests for information from funding agencies may be received up to 90 days post program discharge. Requests greater than 90 days post discharge, must be made through the FOI process, or a renewed consent from client arranged by requestor.
- Confidential information about a client may be provided to Child Protection Services or an appropriate agency as authorised by the Children/Youth Child First and Families Act 2005 to share information.

- Confidential information about a client may be provided to a solicitor or barrister or a Court Registrar only with written consent of the client or a court subpoena.

Release and Transfer of Confidential Information

Releasing Confidential Information

- If client consent to release confidential information is obtained verbally, the staff member must make a file note indicating when and from whom permission was obtained.
- Verbal consent must be followed up by written consent.

Securely Transferring/Transmitting Confidential Information

- QEC staff must ensure that the transmission of confidential data is transmitted/transferred securely in accordance with relevant protocols, program guidelines or work instructions.

Destroying Confidential Information

- All records must be kept for a number of years according to Government regulations (see Critical Records, Access, Retention and Disposal Procedure).
- Paper records containing confidential information for disposal must be placed in locked bin for collection and shredding by a recycling service.
- The selected recycling service must provide guarantees of security of all recyclable materials handled by them or their agents and must be able to supply on request certificates of service/destruction.
- Community Program offices will discard papers of confidential information by shredding or returning to Thomas St office for inclusion in secured paper disposal.
- Computer records that are to be destroyed must be destroyed in a manner in which the information cannot be reconstructed or re-compiled through the ICT department.
- The Systems and Risk Manager or delegate must ensure that computer records are permanently removed, including backup files and data from archive storage.

Environmental policy

QEC is committed to conserving Australia's natural environment and reducing waste and unnecessary costs. To this end it will:

- Dispose of paper records by shredding and recycling at the required time and;
- Progress to electronic document storage wherever feasible.

Related Documents

See also:

1.4.2 Critical Records – Access, Retention and Disposal
1.4.5 Freedom of Information
5.2.4 Equipment Disposal

- Health records Act 2001
- Children, Youth and Families Act 2005
- Information Privacy Act 2000
- Victorian Information Privacy Principles
- Human Rights Charter

Key Legislation, Acts and Standards

PLEASE PLACE A 'Y' IN THE BLANK COLUMN relating to the applicable standards below:- e.g.

1.0 Empowerment	**1.1**	Understanding Rights & Responsibilities	Y
	1.2	Exercising Rights & Responsibilities	

DHS STANDARDS Listing

1.0 Empowerment	1.1	Understanding Rights & Responsibilities	Y
	1.2	Exercising Rights & Responsibilities	Y
2.0 Access & Engagement	2.1	Services Are clear	
	2.2	Services are delivered	
	2.3	Access to Services	
3.0 Wellbeing	3.1	Services Adoption	
	3.2	Services Participation	
	3.3	Goals Documented & Implemented	
	3.4	Reviews, Evaluations & updates	
	3.5	Delivery is in Safe Environment	
4.0 Participation	4.1	Choice & Control of Service Delivery	
	4.2	Community Participation	
	4.3	Maintaining Connections with Family & Friends	
	4.4	Strengthen Culture Connection - Aboriginal/Torres	
	4.5	Strengthen Cultural, Spiritual & Language	
	4.6	Life Skills - Develop Sustain Strengthen	

ISO 9001:2008 Listing

4.0 Quality Management System	4.1	General	
	4.2.1	Doc Requirements General	Y
	4.2.2	Doc Requirements Quality Manual	
	4.2.3	Doc Requirements Control of Docs	
	4.2.4	Doc Requirements Control of records	Y
5.0 Management Responsibility	5.1	Management Responsibility	
	5.2	Customer Focus	
	5.3	Quality Policy	
	5.4	Planning Inc 5.4.1-5.4.2	
	5.5.1	Responsibility & Authority	
	5.5.2	Management Representative	

	5.5.3	Internal Communication	
	5.6	Management Review	
6.0 Resource Management	6.1	Provision of resources	
	6.2	Human resources	
	6.3	Infrastructure	
	6.4	Work Environment	
7.0 Product Realization	7.1	Planning of Product Realisation	
	7.2	Customer-related Processes	
	7.3	Design & development	
	7.4	Purchasing	
	7.5	Production and service provision	
	7.6	Control of monitoring & measuring devices	
8.0 Measurement, Analysis & Improvement	8.1	Measurement Analysis & Improvement	
	8.2	Monitoring & Measurement	
	8.3	Control of non- conforming Product	
	8.4	Analysis of Data	
	8.5	Improvement	

Other Key Legislation, Acts and Standards

Key words: Confidential documents, Privacy information, storage of private information, rights and responsibilities, Human resources, communication