CHERBOURG REGIONAL ABORIGINAL AND ISLANDER COMMUNITY CONTROLLED HEALTH SERVICE LTD (CRAICCHS LTD)

INFORMATION MANAGEMENT SYSTEMS POLICY & PROCEDURE MANUAL

CRAICCHS

Version: June 2018

Author: Kaye Ebbott Consulting

Information Management Systems Policy and Procedure Manual

Prepared June 2018

Author: Kaye Ebbott Consulting

E: kaye.e@optusnet.com.au
P: 0411 551 771

"Assisting community organisations to grow and develop"

VERSION CONTROL AND APPROVAL

Document Approval

The original of this Information Management Systems Policy and Procedure Manual has been endorsed and approved by the Board of Directors at the Board meeting held on:

Date:

Signed:

Name:

Position:

Document Information

This document is stored in a hard copy in the following location:

And electronically in the following location:

LOGIQC

Document Update and Review

Review Date:	Reviewed by:	Adopted date:	Approved by:	Signature:	Next Review Due:
22/05/2018	Veronica Williams and Kaye Ebbott Consulting				

TABLE OF CONTENTS

PREFACE

Information management policies are a key strategic document that will help align information management practices to fulfil the requirements of an information governance framework. It will provide direction and guidance to staff for creating, capturing and managing information to satisfy business, legal and stakeholder requirements, and assigns responsibility across the organisation.

This policy manual:

- Sets out the expected information management practices in the organisation;
- Explains the benefits of good information management;
- Outlines the roles and responsibilities;
- Demonstrates commitment to meeting business, legislative and regulatory requirements;
- Enhance business performance by guiding information management practices, processes and systems that will protect information as an asset;
- Contributes to an environment that values the integrity and accessibility of the information to support the efficient delivery of business outcomes;
- Ensures that information which is trusted, well-described, stored in known locations and is accessible to staff and clients when needed;

Good communication is a fundamental component of ensuring current and relevant information is provided to all stakeholders in the right format, via the right channel and in a timely manner. CRAICCHS will consider how best to communicate with staff and clients, with a combination of both in-person meetings and utilising current information technologies.

Information is an organisational resource to which all staff may have access, except where the nature of the information requires restriction. Access restrictions to information should not be imposed unnecessarily but will protect individual staff/client privacy and sensitive or confidential material. When handling information, staff are to be reminded of the requirements under the *Privacy Act 1988* and the *Information Privacy Act 2009*.

Where the words “CRAICCHS” are used throughout this manual, it is implied that the trading name represents the legal entity of Cherbourg Regional Aboriginal and Islander Community Controlled Health Services Ltd.

OUR VISION

- To provide Aboriginal and Torres Strait Islander people with knowledge, skills and expertise to administer high quality health care;
- To advocate and provide effective and efficient primary health service support to the South Burnett region;
- To facilitate access to comprehensive primary health care, responsive to the needs of our local community.

CRAICCHS aim is for the elimination of inequality in the health and wellbeing experienced by Aboriginal and Torres Strait Islander peoples in the South Burnett region, by sustaining a community-controlled health care service in Cherbourg and surrounding region and ensuring CRAICCHS:

- Operates a sustainable, regional primary health care service with strong community and client support;
- Cooperates with the strategic health initiatives for 'Closing the Gap';
- Establishes partnerships with other providers and with other Aboriginal and Torres Strait Islander organisations; and
- Implements innovative approaches to improve and expand service delivery.

OBJECTIVES

The objectives of the Information Management Systems Policies and Procedures are:

- To ensure the confidentiality of information – data and information assets must be confined to people authorised to access and not be disclosed to others;
- To ensure the integrity of information – keeping the data intact, complete and accurate, and IT systems operational;
- To ensure the availability of information or systems is at the disposal of authorised users when required;
- To ensure CRAICCHS comply with professional and legal obligations and with best practice information security;
- To ensure information is provided to stakeholders by the most effective means.

LEGISLATIVE REFERENCES

- Australian Charities and Not for Profits Commission Act 2012 (Commonwealth)
- Copyright Act 1968 (Commonwealth)
- Corporations Act 2001 (Commonwealth)
- Healthcare Identifiers Act 2010 (Commonwealth)
- Health Services Act 1991 (Queensland)
- Information Privacy Act 2009 (Queensland)
- My Health Records Act 2012 and Rules 2016 (Commonwealth)
- Privacy Act 1988 (Commonwealth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth)
- SPAM Act 2003 (Commonwealth)

STANDARDS AND GUIDELINES

- AS/NZS ISO 31000:2009 Risk management – Principles and guidelines
- Office of the Australian Information Commissioner: *Guide to Securing Personal Information 2015* (Commonwealth)
- RACGP, *Computer and Information Security Standards – For general practices and other office-based practices,* 2nd edition
- RACGP, *Computer and Information Security Templates*
- RACGP, *Standards for General Practices*, 5th edition
- The Australian Information Commissioner, *Australian Privacy Principles Guidelines*, 2015

COMPUTER INFORMATION SECURITY

Policy #4.1

Version: June 2018	**Date of Board Approval:**
Last Review Date:	**Next Review Date:** June 2019

References:

- Financial Management *Policy #13 Fixed Asset Register*
- Information Management Systems *Policy #4.2 Acceptable Use of ICT Systems*
- Corporate Governance *Policy #1.14 Risk Management*
- Corporate Governance *Policy #1.16 Upholding Confidentiality and Privacy*
- Human Resources Management *Policy #2.9 Upholding Confidentiality and Privacy*
- RACGP *Computer and Information Security Standards*

Relevant Documents:

- Risk Management Plan
- Business Continuity Plan
- Asset Register
- Risk Register
- Suppliers Register
- HR D009 V1 - Confidentiality Agreement
- Data Incident / Breach Report

PURPOSE

CRAICCHS has responsibility for a large amount of information held in both electronic and paper-based formats, and it is critical that this information is protected appropriately. CRAICCHS is committed to the preservation of information security through the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk and provide safe, high-quality care and services and good practice management.

The purpose of this policy is to ensure that appropriate measures are put in place to protect organisational and personal information and the ICT systems, services and equipment of CRAICCHS. Data protection and a secure online presence will build client trust, and assist CRAICCHS to meet legal/compliance obligations, such as privacy laws, remain accountable and ensure efficiency.

POLICY STATEMENT

CRAICCHS is committed to providing a secure, yet open information environment that protects the *integrity* and *confidentiality* of information without compromising *availability*.

Confidentiality: ensuring that information is only accessible to those authorised to access it;

Integrity: safeguarding the accuracy and integrity of information and processing methods;

Availability: ensuring that authorised staff have access to information and associated assets when required.
A risk management approach has been adopted by CRAICCHS, where the organisation will identify risks to the ICT systems and data, reduce or manage those risks, and develop a response plan in the event of an IT event. This is designed to maximise opportunities arising from information technologies whilst maintaining strong and effective controls through systems administration to ensure CRAICCHS's information systems remain protected, legally compliant and secure.

To achieve this, CRAICCHS will:

- Establish an appropriate information security culture within the organisation;
- Implement security measures that match the information's value, classification and sensitivity;
- Adhere to all legal requirements;
- Maintain up to date policies and procedures which are accessible to staff and management;
- Ensure that all computers and servers comply with the RACGP *Computer and Information Security Standards*;
- Collect client information in accordance with privacy legislation and securely store that information, with access only available to authorised staff;
- Maintain up to date information regarding staff and securely store that information;
- Archive information securely for the required timeframes, and dispose of information/documentation in an appropriate and secure manner;
- Securely store and regularly back up electronic records, including service delivery information and maintain the computer systems;
- Maintain responsible controls over staff and volunteer use of the internet, email and social media to both access information and to distribute information;
- Ensure the ICT system is effectively managed to protect both the hardware and software from misuse, interference, loss, unauthorised access, modification and disclosure;
- Periodically audit and review information management systems and processes to identify improvements on an ongoing basis and to ensure the organisations information systems operate with a high degree of assurance and integrity.

SCOPE

This policy applies to all CRAICCHS employees, Board of Directors, volunteers, contractors, and any other persons otherwise affiliated but not employed by CRAICCHS, who may utilise CRAICCHS ITC systems with respect to the security and privacy of information. It covers all information communication technology (ICT) as included in the Definitions. This policy covers information created and managed in-house and off-site.

DEFINITIONS

Systems Administrator is the contractor responsible for the administration and maintenance of the CRAICCHS ICT system.

System Users are those who utilise the ICT facilities of CRAICCHS.

ICT means Information Communication Technology. ICT facilities and services are defined as all types of technology (data, voice, video etc.) and associated resources provided or supported by CRAICCHS which relate to the capture, storage, retrieval, transfer, communication or dissemination of information. This includes, but is not limited to desktop computers, mobile electronic devices such as laptops, electronic tablets and handheld devices, mobile phones, removable media (such as CD's, USB flash drives), electronic networks, internet, email, webmail, web services, peripheral equipment such as printers, modems, fax machines, and copiers, and computer software applications (including software that grants access to the internet or email).

ROLES AND RESPONSIBILITIES

CRAICCHS has designated roles for managing computer and information security. CRAICCHS will provide appropriate education and training to these staff members to ensure an appropriate level of knowledge. These roles may be outsourced to ensure appropriate technical knowledge applicable to the role's responsibilities.

Computer Security Coordinator (fulfilled by the General Manager)

The Computer Security Coordinator (General Manager) is responsible for:

- Developing and reviewing (at least annually) documented computer security policies and procedures that are understood by all employees, with input from technical specialists when required;
- Ensuring the existence and testing of the computer business continuity and information recovery plans;
- Monitors and ensures that organisational security policies are being followed, in particular that:
  - Staff are following password security procedures;
  - The routine backup procedures are in place and tested for successful data recovery;
  - Archived data remain capable of being restored in a timely manner;
  - Anti-malware software is installed on all computers and are automatically updated;
  - The computers, especially all servers, are adequately maintained and can deal with fluctuations in power;
  - Clear screen and clear desk policies are followed (i.e. screensavers are activated);
- Raising awareness of information security governance among all employees and ensures staff are aware of any outstanding security issues and regularly reports on security in management meetings;
- Arranging and managing ongoing security awareness training, ensuring that all relevant staff members are provided with appropriate computer security training for their responsibilities;
- Maintaining an up-to-date risk assessment including ensuring the *Asset Register* is up to date (hardware, software, licences, manuals and technical support);
- Ensuring technical advice is sought and acted upon for the installation of protection systems such firewalls;
- Ensuring that information transferred electronically is secure (e.g. uses secure message delivery).

Systems Administrator/Contracted IT Support Personnel

The Systems Administrator are responsible for:

- The administration and maintenance of the ICT systems and network;
- Regularly monitoring the operation and effectiveness of CRAICCHS's ICT security measures to ensure they remain responsive to changing threats and vulnerabilities and other issues that may impact upon the security of information;
- Testing of ICT systems regularly to discover security weaknesses and to test whether networks are operating towards a certain standard;
- Overseeing the practices of system users, and to support skills development as required through provision of IT education and training. All employees are to receive training in virus protection, information security and network induction training, as recorded in the *Staff Training Register*.
- Developing a preventative maintenance schedule to ensure that IT equipment is continuously maintained, and that CRAICCHS has access to appropriate professional IT support.

Responsible Officer

Under the My Health Record system, CRAICCHS will identify the Responsible Officer (RO). This role will usually be filled by the Clinic Manager.

The RO will fulfil the following roles:

- Is registered with the Healthcare Identifiers Service and has authority to act on behalf of the organisation in its dealings with the System Operator of the My Health Record system;
- Primary responsibility for CRAICCHS's compliance with participation requirements in the My Health Record system

Organisation Maintenance Officer

Under the My Health Record system, CRAICCHS will identify the Organisation Maintenance Officer (OMO). CRAICCHS can have multiple OMO's. The OMO needs to be familiar with the IT system used by CRAICCHS.

The OMO will fulfil the following roles:

- Is registered with the Healthcare Identifiers (HI) Service and acts on behalf of the organisation in its dealings with the System Operator of the My Health Record system;
- Primary role is to undertake the day to day administrative tasks in relation to the HI Service and the My Health Record system;
- Will perform tasks related to computer and information security.

Note: the role of the Responsible Officer and the Organisation Maintenance Officer are different and require different responsibilities. It is important to understand the specific responsibilities of each role and it is recommended that these two roles are not performed by the same person.

PROCEDURE

1. Security Governance and IT Control Responsibilities

CRAICCHS ICT system must be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network.

Overall responsibility lies with the General Manager for accountability, monitoring and reporting to demonstrate legal and ethical compliance to sound information security and to ensure that all computer and information security processes are documented and followed.

To contribute to good clinical governance, CRAICCHS will ensure that management identify and understand the legal and professional requirements for the protection of the information for which the service is custodian. CRAICCHS will refer to the RACGP *Computer and information security standards* to help meet our professional and legal obligations and implementing appropriate computer and information security measures, policies and procedures.

The Systems Administrator or contracted IT support personnel will be delegated responsibility for the implementation and maintenance of appropriate data security precautions and effective computer virus software protections across the ICT system. The *"Compliance Checklist for Computer and Information Security"* (contained in the *RACGP Computer and Information Security Standards*) will be completed to assist CRAICCHS assess, achieve and sustain compliance with the standards that comprise good practice in computer and information security.

All Internet and e-mail access connections and structures across the organisation must comply with our security procedures.

2. Developing a Security Culture

CRAICCHS will work with staff to develop a privacy and security aware culture within the organisation, which will include educating staff about the risks to the information systems and the maintenance of policies that direct staff in their management of security risks.

Effective communication, training and education for staff about the risks that the computer and information systems are exposed to is an important aspect of risk management at CRAICCHS. Discussions will also occur at staff meetings. Information security will be incorporated into induction and training to minimise the risk of loss or misuse of information assets.

Policies and procedures relating to information security will be made available to all relevant staff members/management.

Internet and e-mail users will be advised that they are responsible for, and will be held accountable for any data accessed through the use of their CRAICCHS log-on identification password.

2.1. Confidentiality Agreements

CRAICCHS is committed to upholding the privacy of both individual's personal information and the organisation's information, and to comply with the obligations imposed by the applicable privacy legislation. All Board of Directors members, employees and contractors must affirm their commitment to maintaining privacy and confidentiality in relation to CRAICCHS business affairs, including client information, through the signing of the *Confidentiality Agreement*. This forms part of the induction procedures, with a copy of the agreement filed on the employees/Board members personnel file. (Refer to the CRAICCHS *Human Resources Management Policy #2.9 Upholding Confidentiality and Privacy* and *Corporate Governance Policy #1.16 Upholding Confidentiality and Privacy*).

2.2. Code of Conduct

Inappropriate use of computers and the internet can expose the CRAICCHS ICT system to a range of risks. To mitigate this, all system users are provided with clearly documented procedures and rules or guidelines (refer to Information Management Systems *Policy #4.2 Acceptable Use of ICT Systems*. Staff who require access to the ICT system will be required to sign a staff computer use and internet agreement as part of the *Staff Code of Conduct* and *Board* Code of Conduct.

3. IT Administration

3.1. Managing Assets and Equipment

CRAICCHS will manage all physical assets including ICT assets and the security of the information they contain. Assets will be managed in the *Asset Register* on LOGIQC, as per the *Finance Policy #13 Fixed Asset Register*. The management of ICT assets may require assistance from the Systems Administrator, to document the computer hardware, software and information systems used in the organisation. The *Asset Register* will be updated as each new item is purchased by CRAICCHS or new service or application is installed. The Accountant, assisted by the Business Finance Manager, will maintain the *Asset Register*.

Physical assets relating to ICT may include: computer and communications equipment, mobile devices, smart phones, tablet devices, medical equipment that interfaces with the computer systems, backup media and uninterruptible power supplies. Diagrams showing the layout of the network and computers are a useful

resource which CRAICCHS may also include. It could include electronic information assets: databases, electronic files and documents, image and voice files, system and user documentation, business continuity and information recovery plans.

As part of the *Asset Register*, CRAICCHS will record all software licences and assets. Software assets may include: application programs, operating system, communications software, including all clinical management software, as well as email, firewall, backup, virus checking and other utilities. Information recorded may include:

- Software name;
- Serial number;
- Date of purchase;
- Renewal dates if applicable;

Original software media and manuals should be stored securely.

The following information will be recorded by the Systems Administrator:

- Software product code and activation key;
- Number of licences purchased;
- Location of software (i.e. serial number of computer where software is installed).

3.2. IT Service Agreements

CRAICCHS must ensure that anyone who has legitimate access to clinical and/or business information is aware of their obligations to comply with organisational policies related to that information. The General Manager is responsible for the maintenance and management of all service agreements for any aspect of the ICT system. Any service requirements must first be approved by the General Manager. It is recommended that the General Manager seek a legal review of all IT service agreements before the agreement is entered into or renewed.

Contractual arrangements with outsourced technical service providers should include:

- **Data confidentiality**: sensitive clinical and business information must be kept private;
- **Remote access**: if the technical service provider accesses the network remotely, there has to be agreement on what they can or cannot view;
- **Backups and data restoration processes**: length of time for data to be partially or fully restored from backup if data accidentally deleted, information such as back up procedures, how often are the procedures tested and when testing is undertaken must be included in the contract;
- **Response times**: how long will it take the service provider to give phone advice, provide assistance via remote access, do they attend onsite and provide after-hours assistance;
- **Costs**: what are the routine maintenance costs, any additional costs in case of a computer malfunction, do costs differ during office hours and after hours;
- **Regular maintenance**: does the IT service provider undertake monthly server checks;
- **Audit log**: what audit log checking will be undertaken of the network and how will this be reported to CRAICCHS;
- **Secure disposal of information assets**: how are information assets (e.g. backups) disposed of or returned to the organisation;
- **Cloud services**: Where is the data stored and what security assurances are provided:
- **Service provider's business continuity and disaster recovery plan:** does this cover the availability and restoration of both CRAICCHS data and the provider's services that CRAICCHS use;

- **Service provider's guarantee of system availability and quality of service**;
- **Impact of outages:** includes both scheduled and unscheduled by the service provider;
- **Service level agreement compensation:** does this adequately reflect actual damage caused by a breach of the service level agreement, such as unscheduled downtime or data loss;
- **Data integrity and availability:** with the service provider implementing mechanisms such as redundancy and offsite backups to prevent corruption or loss of data, and guarantee both the integrity and the availability of data;
- **Changing service provider:** in the event that CRAICCHS wishes to move data to a different provider, how is access gained to the data, guarantees that CRAICCHS data is permanently deleted from the provider's storage media.

Contact details of all technical service providers will be recorded in the *Suppliers Register* on LogicQC.

4. Risk Assessment of Information Security Risks

CRAICCHS will ensure that it understands and analyses the security risks, vulnerabilities and threats to business and clinical information, including the requirement for effective information security practices by identifying gaps in security and implementing strategies and controls to minimise security risks.

To ensure effective information security, CRAICCHS will undertake periodic, structured risk assessments of computer and information security and implement improvements, treatments and controls as required.

This risk assessment will be undertaken as part of the overall organisational approach to risk management as outlined in the *Corporate Governance Policy #1.14 Risk Management* and CRAICCHS *Risk Management Plan* and documented in the *Risk Register*.

As part of the risk assessment process across the ICT system, CRAICCHS will identify sources of risk, areas of impact, events and their causes and potential consequences. (CRAICCHS *Risk Management Plan, Section 9 Risk Assessment*). A risk analysis will be undertaken (CRAICCHS *Risk Management Plan, Section 10 Risk Analysis)*, which will assist CRAICCHS to better understand and put in place planning to minimise the impact from potential risks, including financial loss, breaches in confidentiality, information integrity and availability and client confidence.

CRAICCHS will categorise ICT (technology) threats into three broad areas:

- human (unintentional and deliberate): for example, the theft of a laptop containing clinical or business information, or inadvertent viewing of a client's information by non-practice staff or another client;
- technical: for example, a hard disk crash or data corruption from a virus;
- environmental: for example, a natural disaster such as a bushfire or flood.

A risk evaluation will assist in making decisions about which risks need treatment and the priority for treatment implementation. Existing controls can be assessed, and any additional required controls can be identified. This will form the plan for improving the security of the computer and information systems.

Selecting the most appropriate risk treatment options for modifying risks involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory and other requirements (refer to *Risk Management Plan, Section 10 Risk Treatment).*

Control selection will be based on cost, ease of use, integration with normal workflow, importance to the organisation, and objective of protection.

4.1. Monitoring and Review

Risk management systems and treatment plans should be monitored and reviewed on an ongoing basis to regularly review whether anything has changed which may impact on the risk issues identified. This will occur when computer equipment and software are updated, new uses of information are undertaken, staff leave or commence, when changes occur to legislation or professional requirements, or following incidents of breaches in information security.

5. Data Breach Response and Reporting

CRAICCHS has obligations under the Notifiable Data Breaches Scheme, My Health Records and Service Agreements to notify individuals, the Australian Information Commission and the My Health Records Systems Operator about eligible data breaches.

Data breaches at CRAICCHS, whether intentional or unintentional, can occur through, but not limited to:

- Loss or theft of laptops, mobile devices, removable storage devices, hard disk drives;
- Unauthorised access of databases from outside the organisation through hacking;
- Unauthorised access of databases from inside the organisation through access or disclosure by employees outside the bounds of their roles and authorisation.

CRAICCHS will ensure that procedures are in place on the detection, action and reporting of breaches of security.

5.1. Identifying Eligible Data Breaches (Privacy Act 1988)

CRAICCHS has an obligation under the Notifiable Data Breaches Scheme to notify individuals and the Australian Information Commission about eligible data breaches.

5.1.1. Identifying an Eligible Data Breach

An eligible data breach arises when the following three criteria are satisfied:

1. There is *unauthorised access* to or *unauthorised disclosure* of personal information, or a *loss* of personal information, that CRAICCHS holds (e.g. a device containing clients' personal information is lost or stolen; a database containing personal information is hacked; personal information is mistakenly provided to the wrong person);
2. This is likely to result in *serious harm* to one or more individuals; and
3. CRAICCHS has not been able to prevent the likely risk of serious harm with remedial action.

Unauthorised access of personal information occurs when personal information that CRAICCHS holds is access by someone who is not permitted to have access (including employees, contractors or external third parties).

Unauthorised disclosure occurs when CRAICCHS, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted under the Privacy Act.

Loss refers to the accidental or inadvertent loss of personal information held by CRAICCHS in circumstances where it is likely to result in unauthorised access or disclosure (e.g. employee leaves unsecured laptop containing personal information on public transport).

Serious harm to an individual may include physical, psychological, emotional, financial or reputational.

Refer to https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches for guidance on deciding whether an eligible data breach has occurred.

5.1.2. Responding to a Suspected or Known Data Breach

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and organisations. Hence, there will be no single way of responding to a data breach, but rather, each breach will be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

At any time including immediately and during an assessment, CRAICCHS will take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the notification obligations may not apply.

Generally, the actions taken following a data breach will follow the following steps:

Step 1: Contain the breach

Once CRAICCHS has discovered or suspects that a data breach has occurred, the first step is to immediately contain or limit the breach so that no further damage can be done. Depending on the nature of the breach, the following may apply:

- Stop the unauthorised practice;
- Recover the records;
- Isolate the system or disconnect from the internet if this is likely where the breach occurred. If it is not practical to shut down the system (or it might result in a loss of evidence) then suspend user access to the records affected, or suspend a specific user's access, or address weaknesses in physical or electronic security.

Step 2: Assess suspected Data Breaches

Assess:

If CRAICCHS is **aware of reasonable grounds to believe** that there has been an eligible data breach, it must promptly notify individuals at risk of serious harm and the Australian Information Commission about the eligible data breach (refer to Step 3: Notifying about an Eligible Data Breach).

If CRAICCHS **has reason to suspect** that an eligible data breach may have occurred, the General Manager or delegate will undertake a reasonable and prompt assessment to determine if the data breach has occurred and is likely to result in serious harm to any individual affected. This may require technical assistance from the Systems Administrator as the person will need experience in evaluating the cause and be able to make recommendations.

Refer to https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach for resources to assist with "*assessing a suspected data breach*". CRAICCHS will take all reasonable steps to complete the assessment as quickly as possible, but within a maximum timeframe of 30 calendar days.

If, during the course of the assessment, it becomes clear that there has been an eligible breach, CRAICCHS will promptly comply with the notification requirements.

An assessment may be a three-stage process:

1. **Initiate**: decide whether an assessment is necessary and identify which person will be responsible for completing it;
2. **Investigate**: quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts;
3. **Evaluate**: make a decision, based on the investigation, about whether the identified breach is an eligible data breach (refer to *Section 5.1.1 Identifying an Eligible Data Breach*).

Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made. A Data Incident / Breach Report form will be completed.

Take remedial action:

Where possible, CRAICCHS should take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed or changing access controls on compromised client accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required, and entities can progress to the review stage (step 4).

Step 3: Notifying about an Eligible Data Breach

Once CRAICCHS has reasonable grounds to believe there has been an eligible data breach, CRAICCHS must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Australian Information Commission (Commissioner) and notify individuals of this statement.

CRAICCHS will consider 3 options for notifying individuals at risk of serious harm, depending on what is practicable (considering time, effort and cost of notifying individuals):

- Notify all individuals whose personal information was part of the eligible data breach;
- Notify only those individuals at risk of serious harm; or
- Publish notification (if neither of the other options above are practicable, for example).

Further information in relation to how to notify and what information needs to be included in the statement can be found at:

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach and

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/what-to-include-in-an-eligible-data-breach-statement

CRAICCHS must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of the eligible data breach. The statement can be lodged to the Commissioner through an online form:

https://forms.uat.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

Notification can be an important mitigation strategy that has the potential to benefit both CRAICCHS and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will not always be an appropriate response to a breach. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

Step 4: Review

Once the immediate steps are taken to mitigate the risks associated with the breach, CRAICCHS will take the time to investigate the cause and consider whether to review the existing prevention strategies. This may include:

- A security audit of both physical and technical security;
- A review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that;
- A review of employee selection and training practices.

CRAICCHS will review and lean from the data breach incident to improve its personal information handling practices and reduce the chance of reoccurrence. If any updates are made following a review, staff will be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.

5.2. Breaches Under the Information Privacy Act 2009 (Queensland)

Under the Service Agreement with the Department of Communities, Child Safety and Disability Services (the Department), CRAICCHS must make every reasonable effort to notify the Department immediately upon becoming aware of any breach of the *Information Privacy Act 2009* or the privacy obligations under the Service Agreement. A breach of privacy may involve the privacy of a single individual or a general loss of data may occur. Notification of any breach will be in addition to CRAICCHS taking its own remedial action of the breach.

In relation to protection of personal information, CRAICCHS must immediately notify the Department if:

- The organisation knows or suspects that confidential information has been disclosed without the authorisation of the Department;
- There has been any breach of protection of personal information;
- The organisation becomes aware that disclosure of personal information in relation to any child subject to the *Child Protection Act* or the *Youth Justice Act*, is made or may be required under law.

5.3. Mandatory Data Breach Notification – My Health Record System

5.3.1. What is a Data Breach?

Under the *My Health Records Act 2012*, as a registered healthcare provider organisation, CRAICCHS has mandatory data breach notification requirements. There are three types of data breaches:

1. A person has or may have contravened the *My Health Records Act* through unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record;
2. Any event that has, or may have, occurred that compromises, may compromise, has compromised or may have compromised the security or integrity of the My Health Record system; or
3. Any circumstances that have, or may have arisen, that compromise, may compromise, have compromised or may have compromised the security or integrity of the My Health Record system.

CRAICCHS must report the breach when they become aware that such a data breach has, or may have, occurred, and the data breach directly involved, may have involved or may involve CRAICCHS.

5.3.2. Reporting Requirements

The notifiable breach must be reported to the OAIC and the System Operator.

CRAICCHS must report a notifiable data breach as soon as practicable after becoming aware of the breach. If there is uncertainty about whether the breach is notifiable under the *My Health Records Act*, CRAICCHS should report the breach.

Reporting of notifiable data breaches should preferably be in writing, although notification by other means will also meet the requirements set out in the My Health Records Act. In urgent cases, the OAIC encourages preliminary notification followed by more detailed notification.

The following notification contacts are available:

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218, Sydney
NSW 2001

Facsimile: 02 9284 9666

Information to include in the notification can be found at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system#part-2-reporting-requirements-for-registered-healthcare-provider-organisations-rros-rpos-and-registered-contracted-service-providers

5.4. Other Considerations of a Data Breach

Where a known eligible data breach has occurred, the General Manager is to notify the Board of Directors.

Where theft or criminal activity is suspected, the General Manager is to notify the police.

5.5. Summary – Data Breach Response Process:

DATA BREACH OCCURS
Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.

↓

KEY STEPS IN RESPONDING TO A DATA BREACH		
Step 1:	**Contain the breach to prevent any further compromise of personal information**	• Take immediate steps to contain the breach • Designate person/team to coordinate response
Step 2:	**Assess the data breach by gathering facts and evaluating the risks, including potential harm to affected individuals**	• Consider what personal information is involved • Determine whether the context of the information is important • Establish the cause and extent of the breach • Identify what is the risk of harm
Step 3:	**Consider breach notification**	• Risk analysis on a case-by-case basis • Not all breaches necessarily warrant notification

↓

SHOULD AFFECTED INDIVIDUALS BE NOTIFIED	
Where there **is a real risk of serious harm**, notification may enable individuals to take steps to avoid or mitigate harm. Consider: • Legal/contractual obligations to notify • Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities.	**Process of Notification** • **When?** - as soon as possible • **How?** - direct contact preferred (mail/phone) • **Who?** - entity with the direct relationship with the affected individual • **What?** - description of breach, type of personal information involved, steps to help mitigate, contact details for information and assistance.

↓

SHOULD OTHERS BE NOTIFIED?			
• **Office of the Australian Information Commissioner** • My Health Records • Police/Law Enforcement • Professional or Regulatory Bodies • Other agencies or organisations affected by the breach or contractually required to notify	→	**Step 4:**	**Review the incident and take action to prevent future breaches** • Fully investigate the cause of the breach • Consider developing a prevention plan • Option of audit to ensure plan implemented • Update security/ response plan • Make appropriate changes to policies and procedures • Revise staff training practices

6. Virus Protection and Software Security

Electronic communications are potential delivery systems for computer viruses, which have the potential to seriously damage CRAICCHS ICT systems. To protect the organisational resources against intrusion by viruses and other malware, CRAICCHS has installed and uses anti-virus products on all computers that have internet access, including servers and networks.

The minimum requirements for antivirus protection are as follows:

- The anti-virus product shall be operated in real time on all servers and computers. The product shall be configured for real time protection;
- The anti-virus library definitions shall be set to update automatically to ensure updates of at least once per day;
- Anti-virus scans shall be set to run a minimum of once per week on all user-controlled workstations and servers;
- No one should be able to stop anti-virus scans, disable bypass or adjust settings except for the Systems Administrator;

The Systems Administrator will be responsible for:

- Ensuring that the latest versions of software and applications are in use across the organisation;
- Removing or disabling unneeded software, operating system components and functionality to reduce its vulnerability to attack and make it harder for malware to run or for an attacker to gain access.
- Ensuring that appropriate network security controls are in place, including the use of firewalls which control the incoming and outgoing network traffic, and software applications, that monitor network or system activities for malicious activities, anomalous behaviour, or policy violations (refer to *Section 7 Other Computer Network Perimeter Controls*).

As outlined in *Information Management Systems Policy #4.2 Acceptable Use of ICT Systems*, staff will be educated and trained:

- Not to respond or click on links in emails from unknown sources;
- To only open attachments where the source of the file is known;
- To ensure all files downloaded from the internet are scanned for viruses;
- How to respond to pop-up messages from antivirus software;
- To report unusual activity on the system, as no malware software is 100% effective.

All data, programs and files which are downloaded electronically or attached to email messages should be automatically scanned by an anti-virus program before being launched, opened or accessed.

Employees are not to open any downloaded files, emails or attachments that the employee is not expecting or that look suspicious. In the event that an employee receives any files that they suspect contain a virus, it should be reported immediately to the General Manager via voice communication who will contact the Systems Administrator.

If staff work on a home personal computer and bring files to work on a USB or other portable device, the data must be checked for viruses prior to the files being opened on an office computer. All disks/files received from external sources, including by e-mail, are to be virus checked before opening.

7. Other Computer Network Perimeter Controls

7.1. Firewalls

Firewalls will be installed to check messages coming in to and out of the CRAICCHS network and block unauthorised access to the network. This will add a layer of protection between the organisation's computers and the internet. The firewalls will be properly configured and periodically tested (with testing dates recorded) to ensure that they are still working and updated as required. This will be the responsibility of the Systems Administrator. The configuration of firewall devices will be recorded by the Systems Administrator, as outlined in *Section 3.1 Managing Assets and Equipment*.

7.2. Secure Remote Access

Secure remote access between a CRAICCHS remote computer and the server will be provided. Only management have this direct access, with staff requiring management approval for remote access and to take a laptop off site

7.3. Content Filtering

CRAICCHS will use software programs to filter email (such as filtering for spam).

7.4. Wireless Networks

CRAICCHS will ensure that additional security measures are in place across any wireless networks (i.e. Wi-Fi). CRAICCHS will obtain technical advice from the Systems Administrator on how best to keep Wi-Fi (or Bluetooth) enabled equipment and information they hold secure. Where appropriate, Wi-Fi devices must have encryption set up to ensure the confidentiality of information.

Staff will be alerted to take care when using devices in public places to avoid information being sighted, as well as when connecting via open or unsecured public networks.

8. Managing Access

8.1. Access Control

Control of who has access to business and clinical information is essential to the protection of all electronic data and information systems. Access to systems and information shall be restricted to authorised users who have legitimate business needs to access the information to enable them to perform their role.

Computer systems will be set up so that staff have appropriate levels of access to files and information to match the individual user role. This will be controlled through passwords to restrict access to specific files. This will include the ability to create and edit certain files, read only access to some files and no access to certain confidential files. Staff will also be conscious to save files in the appropriate format (eg: Read Only) and where necessary identify staff who should have access. Restricting access reduces the opportunity for accidents and errors.

System access privileges will be changed when staff change position within the organisation. It is the responsibility of the General Manager to ensure this is undertaken by emailing the Systems Administrator who will make the necessary changes and email back confirmation, which is filed for recording purposes.

Staff will receive appropriate training in the relevant computer software and the potential risks before access and passwords are provided.

8.2. Passwords & User-ID Maintenance

CRAICCHS has systems in place to protect the security of data held on the ICT system. System access will be via unique user-ID and require authentication in the form of a secure password. Where access to a computer (including a fixed or mobile device) at CRAICCHS and/or its networks is required by any personnel – either a part-time, full-time, casual, contractor or visiting health professional - an appropriate user-ID access will be provided.

The following guidelines will be used by CRAICCHS in managing passwords:

- All staff create their own 'strong' login password(s) for access and be responsible for keeping them secret and secure;
- Logins are not shared (i.e. people in the same role do not use the same username and password);
- Staff are to have individual access credentials for each business system;
- Passwords do not use familiar and family names;
- Dates of birth are not used;
- Passwords are not reused;
- Passwords are not disclosed to anyone and others are not allowed to use your login;
- Passwords are not written down where they can be obtained by other staff or people who have access to the premises (i.e. not attached to screens);
- Default user account passwords must be changed;
- Generic passwords will not be used;
- Passwords are changed periodically, with automatic electronic alerts;
- The system administrator's password should never be divulged to anyone who is not authorised.
- Passwords should be changed immediately if they have been or are suspected of having been compromised.

For medico legal reasons, and to provide evidence of items billed in the event of a Medicare audit, staff, especially nurses always log in under their own passwords to document care activities they have undertaken.

Password protected screen savers are installed on every computer at CRAICCHS and will protect the computer to prevent unauthorised access to computers.

8.3. Password/User ID Management

The Systems Administer is responsible for:

- Issuing of user-ID's with these recorded by the Systems Administrator;
- Creating and removing users/access on each information system/program;
- Resetting user passwords, via an email request from the General Manager, which is retained as a record of the request.

A staff member's access will be removed when they are no longer working at the organisation, with password and remote access logins decommissioned. This is the responsibility of the Systems Administrator, via an email request from the General Manager, which is retained as a record of the request.

8.4. Auditing

Monitoring on all CRAICCHS ICT systems will be implemented by the Systems Administrator to record logon attempts (both successful ones and failures) and exact date and time of logon and logoff. The Systems Administrator shall maintain a process for providing reports of invalid log on attempts upon request from the General Manager as required. The Systems Administrator shall maintain a process for detecting and reacting to systematic attacks on the server system of CRAICCHS.

9. Business Continuity and Information Recovery

CRAICCHS is implementing documented and tested plans for business continuity and information recovery. This is a critical element of our computer and information security and contributes to good governance processes within the organisation. The organisation's *Business Continuity Plan* ensures continued operations when computer system failure occurs, either through an internal system malfunction or from an external event or source.

This plan encompasses all critical areas of clinical operations such as making appointments, billing clients and collecting client health information.

The plan is tested on a regular basis to ensure backup protocols work properly and that the practice can continue to operate in the event of a computer system failure.

The A*sset Register* is an integral part of the *Business Continuity Plan* as it provides much of the essential information required to recover the computer systems quickly and efficiently (refer to *Section 3.1 Managing Assets and Equipment*).

10. Back-Up of Data

10.1. Backup Frequency and Type

To protect data and to be sure it is not lost and can be recovered promptly in the event of an equipment failure, intentional destruction of data, or disaster, CRAICCHS has implemented and practices regular and automated systems backups on a daily, weekly and monthly basis and stores a copy of data backups at an offsite location.

Any changes to data and files should be backed up, including practice management and clinical systems data as well as other relevant documents, email files, user profiles including desktop settings and internet favourites and bookmarks. This policy applies to all software installation packages and data owned and operated by the organisation including but not limited to accounting files, invoicing systems, letters and email, information and resources and website files.

Business and clinical data backups must be performed daily, while system backups can be performed less frequently as the operating system and software change less frequently.

It is important for CRAICCHS to keep a correct and current copy of the computer practice and policy procedure manual offsite so that if there is a systems failure, there is ready access to the restoration and business continuity procedures.

10.2. Backup Reliability

The System Administrator is responsible for ensuring this policy is in practice at all time and that the back-up system is regularly tested to ensure that it restores all information correctly and promptly if there is an incident. The General Manager is responsible for checking and signing off on data backups a minimum of once per month.

10.3. Backup Restoration

In the event that data restoration is required after the system/server has become inoperable, the Systems Administrator is responsible for rebuilding the system. The restoration process will be periodically tested and validated.

The restored data will be visually checked by an authorised person (such as the Clinic Manager), with one such method being to ensure the last client entry from the previous day is present on the restored system.

The process for backup restoration will be documented, so that if required the backup can be used to restore all or part of the clinic data and programs.

10.4. Backup Media

CRAICCHS will seek technical advice to ensure the most appropriate backup software and hardware for the organisation circumstances is chosen.

CRAICCHS will ensure that the backup is not accessible across the normal network from the internet.

10.5. Backup Storage

All backups are stored offside by the Systems Administrator.

10.6. Legacy Systems Data Storage

CRAICCHs will ensure that archive backups (weekly, monthly and yearly backups) can be read in the future by current hardware. The Systems Administrator will be responsible for checking and transferring archive backups to current backup media when required prior to hardware/software updates and new technology.

11. Cloud Computing

11.1. Cloud Computing Administration

CRAICCHS will utilise cloud computing services where appropriate for storing data and software. Cloud services may not be appropriate for all applications and classifications of data. Where cloud services are used, the cloud services must be fit for purpose and used appropriately. The benefits to CRAICCHS include IT cost savings, business continuity and improved business outcomes and flexibility.

CRAICCHS will seek assistance from the Systems Administrator in establishing, maintaining and reviewing cloud computing services. Use of cloud computing services for business purposes must be formally authorised by the General Manager. The Systems Administrator will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing service provider.

In evaluating cloud services and their use for data storage, CRAICCHS will:

1. **Assess** information against legislative and regulatory requirements;
2. **Evaluate** the market for cloud services;
3. **Determine** the suitability of the cloud service against the information requirements;
4. **Procure** and implement the cloud service;
5. **Monitor** the cloud service for performance and compliance;
6. **Review** the cloud service for ongoing benefits realisation.

The General Manager, with advice from the Systems Administrator, will decide what data may or may not be stored in the cloud.

The use of cloud computing services must comply with:

- CRAICCHS Policies and Procedures;
- All laws and regulations governing the handling of personally identifiable information, organisational financial data or any other data owned or collected by CRAICCHS.

11.2. Cloud Computing Security and Risk Assessment

CRAICCHS will carefully consider information security risks, which will vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud service provider has implemented their specific cloud services.

A risk management process will be used to balance the benefits of cloud computing with the security risks associated with CRAICCHS handing over control to a provider. Refer to *Section 4 Risk Assessment* for the procedure to follow in undertaking a risk assessment. A risk assessment will be undertaken to determine the viability of using cloud computing services and to identify and manage relevant information security risks associated with cloud computing.

When considering moving to a cloud solution, CRAICCHS, with advice from the Systems Administrator should consider:

- **Quality** - does the cloud solution meet stakeholder needs and fit for purpose;
- **Financial** - does the cloud solution provide value for money;
- **Organisational** - does the cloud solution work within the organisation's culture;
- **Integration** - can the cloud solution meet objectives without business or technical integration difficulties;
- **Compliance** - does the cloud solution comply with CRAICCHS's legal, regulatory and policy obligations;
- **Business continuity** - can the cloud service provider recover from outages or disaster situations; what is the impact of an outage; ensure the availability of data in the event of any situation;
- **External** - is the Cloud service provider's performance adequate.

11.3. Cloud Computing Access

Access to cloud computing will be restricted to those authorised staff who require access to this information in order for them to fulfil the requirements of their role.

Access to cloud services will be via a login-ID and password, managed by the Systems Administrator. Users that are provided access to cloud services must comply with CRAICCHS policies, including *Information Management Systems Policy #4.2 Acceptable Use of ICT Systems*, and any other terms of use notified by CRAICCHS in relation to specific cloud services.

The General Manager may suspend or terminate access to cloud services at any time.

11.4. Permissible Content

Any content loaded onto cloud services must:

- Comply with CRAICCHS *Information Management Systems Policy #4.2 Acceptable Use of ICT Systems;*
- Comply with the acceptable use policy applicable to the cloud services; and
- Comply with all laws, not infringe any third party's intellectual property rights and not be offensive.

A cloud service provider's use policy must be reviewed to ensure that any data or content CRAICCHS transfer onto the cloud does not violate such policy.

12. Mobile Electronic Devices

CRAICCHS has processes in place to ensure the safe and proper use of mobile electronic devices in accordance with organisational policies and procedures for managing information security.

Mobile devices include any device used to contain information or enable access to sensitive information. Examples may include but are not limited to laptop computers, tablet devices, notebook PCs, USB flash drives, removable hard drives, mobile phones (particularly 'smart phones'), personal digital assistants (PDA), and backup media such as drives, tapes and discs. Examples may also include portable electronic clinical equipment.

All of these devices present a higher risk of being lost, stolen or left unsecure, which increases the risk of data inadvertently ending up with unauthorised people. CRAICCHS will ensure computer and information security measures include all mobile devices.

12.1. USB Devices

The use of USB devices will be strictly controlled within CRAICCHS as the ad hoc transfer of information poses security risks. Confidential or client information will not be transferred or stored on a USB device. USB's will not be left in an unsecured environment.

12.2. CRAICCHS Owned Devices

Security for all mobile devices will be increased using passwords and encryption where appropriate. Employees who are issued mobile devices will be required to lock them with a unique PIN in case of theft or loss. When not in use these devices should be placed in a secure location.
Bulk downloading or transfer of information using portable devices will be strictly controlled and audited.

Technical advice may be sought on how mobile electronic devices can be further secured.

13. Physical Facilities and Computer Hardware, Software and Operating System

CRAICCHS manages and maintains our physical facilities and computer hardware, software and operating system with a view to protecting information security.

13.1. Physical Protection

CRAICCHS computers and the network are valuable assets (including information stored on them), therefore, access will be limited to authorised personnel. This will also protect against theft.

The physical location of the server is a key consideration, with it contained in a locked, safe place with password access limited to key members of the organisation including the General Manager and Systems Administrator.

Desktop and laptop computers and other portable devices will always be kept physically secured. Software, disks and backup media will be locked away to limit physical access.

CRAICCHS will also consider environment protection, including positioning computers, backup media and other components of the network where they are not subject to excessive heat. All computers will be kept reasonably dust free. CRAICCHS will consider the location of the server in relation to fire hazards, water damage, humidity and air temperature, with the room monitored for excessively high temperatures which may lead to equipment failure.

All removable computer equipment will be secured from theft or damage, with laptops and similar equipment locked away at night if left on the premises. Specific consideration to security will be given where equipment is in areas that are frequented by clients and visitors to the workplace.

13.2. Uninterruptible Power Supply (UPS)/Generator

CRAICCHS has installed a generator for emergency power in the event of a power outage. The generator is routinely tested by a qualified electrician to ensure it is in working order in the event of a power outage.

The emergency power supply will allow computers (especially servers) to shut down normally when the main power is lost. This will ensure that data being processed is not lost or corrupted while the blackout occurs and will also help with power surges that can cause hardware damage.

A surge protector is installed on the power supply to the server as well as workstations.

13.3. Secure Disposal

CRAICCHS ensures appropriate and secure disposal of old or decommissioned computer equipment, and importantly, any data storage media especially hard disks. Disks and backup media should be securely erased (overwritten), disposed of using the contracted I.T. company or physically destroyed.

To reduce the potential loss or theft of equipment and assets, all removal from the CRAICCHS premises is formally recorded to minimise theft and loss.

All reasonable steps will be taken to securely destroy paper-based confidential data and information, such as shredding.

13.4. Confidentiality

Clients should not be able to view the clinical record of another person (e.g. the client previously consulted). Receptionists need to be careful that clients do not have inappropriate visual access to any information on computer screens at the front desk.

All practice team members are made aware of how they can keep sensitive information from being inadvertently viewed. This will form part of staff training and induction procedures for applicable staff.

CRAICCHS computers will utilise password protected screensavers, set so that the user has to enter their password to log back into the system. Clinic staff must also log off when leaving terminals.

To avoid accidental and unauthorised viewing of documents, CRAICCHS will use a clear desk policy for confidential material. This means at the end of each day each clinic staff clears their desks of all confidential documents, notes and media. In addition, all documents should be removed from printers and fax machines immediately after being copied, sent or received.

13.5. System Maintenance

The Systems Administrator is responsible for systems administration and maintenance. The Systems Administrator is to establish a preventative maintenance schedule to ensure that IT equipment is continuously maintained, and that the organisation has access to appropriate professional IT support.

The preventive maintenance schedule is to be approved by the General Manager. The annual budget will include a budgetary forecast for IT maintenance and support.

13.6. Software Maintenance

CRAICCHS will ensure maintenance work on the computer system software on an ongoing basis, with monitoring such as:

- Check for installation of unauthorised programs;
- Restricting user access to avoid full administrative access, which will limit the ability of user to install additional applications and programs;
- Keep software up to date;
- Software configuration: install and maintain software in accordance with the vendor's guidelines to ensure security is maintained

CRAICCHS will seek technical advice to ensure the efficient functioning of the computer software.

13.7. System Failure and Corrective Action

The Systems Administrator is responsible for all equipment maintenance problems and system failures. In the event of any computer equipment problem or system failure, the applicable Program Manager/Coordinator is to be notified, who will record the details of the problem/failure and contact the Systems Administrator.

Staff are to notify the full details of what operations were being performed prior to the system failure or breakdown and the exact error message details (if applicable) that appeared on the screen.

The Program Manager/Coordinator or General Manager will assess the urgency of the situation of the problem or failure and take appropriate action.

ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS

Policy #4.2

Version: June 2018	**Date of Board Approval:**
Last Review Date:	**Next Review Date:** June 2019

References:

- Human Resource Management *Policy #2.6 Disciplinary Action and Poor Performance*
- Human Resource Management *Policy #2.8 Sexual Harassment, Discrimination and Bullying*
- Human Resource Management *Policy #2.17 Use of Property and Equipment Policy*
- Human Resource Management *Policy # 2.18 Copyright and Intellectual Property*

Relevant Documents:

- HR D012 V2 - Newstart Checklist Form
- HR D011 V1 – Staff Code of Conduct
- CG D001 V1 – Board Code of Conduct
- HR D009 V1 – Confidentiality Agreement

PURPOSE

This policy is designed to guide staff in the acceptable use of computer and information systems and networks provided by CRAICCHS. Access to the internet and email is provided to CRAICCHS employees for the primary purpose of assisting them in the efficient and professional delivery of services. This policy defines acceptable behaviour expected of users and ensures the use of electronic media is legal, ethical and consistent with the values of CRAICCHS. CRAICCHS supports the right of staff to have access to reasonable personal use of the internet and email communications in the workplace.

POLICY STATEMENT

Information Communication Technology (ICT) systems and services are provided by CRAICCHS to users to conduct organisational pursuits. Users must take responsibility for using ICT systems and services including internet and email in an ethical, secure, responsible and legal manner, having regard for the mission and values of the organisation and the privacy, rights and sensitivities of other people. CRAICCHS may at any time take appropriate action to establish if organisational ICT systems and services are being misused. Any employee who breaches this policy may be subject to disciplinary action up to and including dismissal.

SCOPE

This policy applies to all users of CRAICCHS ICT, including all CRAICCHS employees, volunteers, Board of Directors members, visiting health professionals engaged by CRAICCHS, agents and contractors.

DEFINITIONS

ICT means Information Communication Technology. ICT facilities and services are defined as all types of technology (data, voice, video etc.) and associated resources provided or supported by CRAICCHS which relate to the capture, storage, retrieval, transfer, communication or dissemination of information. This includes, but is not limited to desktop computers, mobile electronic devices such as laptops, electronic tablets and handheld devices, mobile phones, removable media (such as CD's, USB flash drives), electronic networks, internet, email, webmail, web services, peripheral equipment such as printers, modems, fax machines, and copiers, and computer software applications (including software that grants access to the internet or email).

Systems Administrator is the officer or contractor responsible for the administration and maintenance of CRAICCHS ICT system.

Users are those who utilise the ICT facilities of CRAICCHS.

PROCEDURE

1. Access and Acceptable Use

The primary purpose for which CRAICCHS provides employees access to the ICT system is to assist them in carrying out their duties with CRAICCHS. Employees should have access to the internet for email and research purposes only if it supports their work role.

The CRAICCHS ICT systems are tools to be used for CRAICCHS related purposes only unless otherwise authorised in this policy. Their use must be lawful, ethical and appropriate, in accordance with CRAICCHS values, policies and *Code of Conduct*, and with all applicable State and Commonwealth legislation and regulations.

The following outlines expectations with respect to acceptable use of CRAICCHS IT services, equipment and information by all employees and volunteers.

1.1. Information Systems

- Computer terminals should be locked when not in use, logged out and closed down at the end of each day.
- Employees must not allow family members or other unauthorised individuals to access the CRAICCHS ICT System. This includes the use of CRAICCHS internet access devices such as modems and mobile phones.
- Obtaining unauthorised access to electronic files of other people or to email or other electronic communications of others, is not permitted and may constitute a criminal offence under legislation.
- Use of CRAICCHS computer networks and internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems.
- Using CRAICCHS ICT systems to access, create, view, transmit or receive racist, sexist, threatening or otherwise objectionable or illegal material is strictly prohibited and violates CRAICCHS *Human Resource Management Policy #2.8 Sexual Harassment, Discrimination and Bullying*. Employees must abide at all times with all state and commonwealth legislation in their internet usage, particularly in relation to sexual harassment, discrimination, bullying and privacy.
- As part of the CRAICCHS Induction process, employees will be provided with information on acceptable use of ICT Systems, as included in the CRAICCHS *Newstart Checklist Form*. All employees must affirm their commitment to maintaining privacy and confidentiality in relation to business or personal information, including client information, through the signing of the *Confidentiality Agreement*.

1.2. Passwords

System access will be via user-ID and password. Where access to a computer at CRAICCHS and/or its networks is required by any personnel – either a part-time/full-time/casual or visiting health professional, an appropriate password access will be provided.
The confidentiality of passwords is to be maintained by all employees and users of the CRAICCHS ICT systems. Password security is critical to the security of CRAICCHS as well as ensuring privacy for our clients. This means that passwords should not be:

- Disclosed to any other unauthorised person (even over the phone) and should not be written down or attached to screens;
- Sent through the mail;
- Included in a non-encrypted stored document;
- Revealed or hinted at on a form on the internet;
- Retained using the 'Remember Password' feature of the application programs such as Internet Explorer, your email program or any other program;
- If anyone asks for your password, refer them to the General Manager.
- Passwords do not use familiar and family names;
- Dates of birth are not used;
- Passwords are not reused;
- Other staff are not allowed to use your login;
- Logins are not shared (i.e. people in the same role do not use the same username and password).

Employees must change their password if they know or suspect that their password has been compromised. This **must** also be reported by the employee to their manager. Any abuse of passwords will be considered as serious misconduct and disciplinary action may be taken as outlined in the Human Resource Management *Policy #2.6 Disciplinary Action and Poor Performance.*

Password protected screen savers are installed on every computer at CRAICCHS and will protect the computer within 10 minutes of no user activity. Computers should not be left unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. Users can press the CTRL-ALT-DEL keys and select 'Lock Computer' to ensure maximum data protection.

2. Equipment

When using CRAICCHS IT equipment, employees and volunteers must adhere to the *Human Resource Management Policy #2.17 Use of Property and Equipment Policy*.

3. Internet and Information Technology

The Internet and Information Technology environment of CRAICCHS is intended to allow for the creation, access and transmission of information pursuant to achieving the objectives of CRAICCHS. Staff are expected to demonstrate professional integrity and confine personal usage to a minimum.

It is recognised that there may be times when staff need to use the internet for extended personal use. In these situations, it is a requirement that the employee advise and negotiate this with their manager beforehand in order to obtain the manager's approval. In these situations, the time spent on the internet replaces all or part of an employee's break/s for that day, or that they adjust their timesheet accordingly for that day.

3.1. Limited Personal Use of Internet Facilities

CRAICCHS permits reasonable personal use of internet facilities which is infrequent and brief, provided that this use is lawful and does not:

- Interfere with the performance of the employee's work duties or the duties of others; or
- Interfere with the delivery of services to CRAICCHS clients; or
- Interfere with the operation of CRAICCHS or compromise the reputation or public image of CRAICCHS; or
- Breach any CRAICCHS policy or procedure.

3.2. Guidelines for the Use of Internet Facilities

The following guidelines apply to all employees and volunteers:

- Internet usage by all employees is to be consistent with the CRAICCHS *Code of Conduct;*
- Internet time should be minimised to keep costs as low as possible and web browser applications should be closed when not in use;
- The internet is not to be used to access, download, send, search or post inappropriate, offensive or criminal material. Using the internet in a manner that may cause offence or bring CRAICCHS into disrepute is prohibited and may result in disciplinary action;
- Installation of links to social interaction tools and web sites such as Facebook, YouTube, MSN Chat, MySpace, etc. is not allowed, unless with prior consent of the General Manager. Installation of peer-to-peer (P2P) file-sharing network programs such as LimeWire, is strictly forbidden;
- Employees must not undertake internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities;
- Large volumes of data must not be downloaded or transmitted (a large file is defined as equal to or greater then 50mbits in size);
- Employees must not gain, or attempt to gain unauthorised access to any network, CRAICCHS information, communications computing facility or resource through the use of the CRAICCHS information technology environment or attempt to disable or compromise the security of information contained on CRAICCHS computers. Employees must not attempt to bypass, evade or otherwise negate any controls that CRAICCHS may implement in support of the secure and effective operation of its ICT system;
- Web browser security settings are not to be changed without authorisation;
- Treat any network that CRAICCHS does not control as insecure, particularly public WI-FI;
- Employees must not access websites which puts CRAICCHS at risk of viruses, compromising copyright or intellectual property rights. This includes abiding by all copyright laws when downloading, uploading and copying or dealing with any software/applications or any other material from the internet (refer to *Human Resource Management Policy # 2.18 Copyright and Intellectual Property, Section 4 Software Licensing and Copyright*);
- Employees should check for the padlock symbol in the web browser address bar and 'https' at the start of the website address when visiting sites, which indicates a secure site;
- Employees should first check a website they visit to ensure they do not have to pay for material they are trying to access or download. If there is a cost associated for legitimate, work-related material, the employee must first seek permission from their supervisor before proceeding with any download;
- Any costs associated with personal use of the CRAICCHS electronic media may be recouped from the employee;
- The internet must not be used by employees to exchange any confidential or sensitive information held by CRAICCHS, unless in the authorised course of their duties.

4. Email Usage

Email is a business communication tool and users are expected to utilise this tool in a responsible, respectful effective and lawful manner. Unauthorised or inappropriate use of the CRAICCHS email system may result in disciplinary action up to and including summary dismissal and will be dealt with according to the *Human Resource Management Policy #2.6 Disciplinary Action and Poor Performance.* Staff are expected to demonstrate professional integrity and confine personal usage to a minimum.

4.1. Personal Email Use

CRAICCHS permits reasonable personal use of email facilities (i.e. correspondence to family / friends) provided that this use is lawful and does not:

- Interfere with the performance of the employee's work duties or the duties of others; or
- Interfere with the delivery of services to CRAICCHS clients; or
- Interfere with the operation of CRAICCHS or compromise the reputation or public image of CRAICCHS; or
- Breach any CRAICCHS policy or procedure.

The use of emails for personal use must be accepted as a privilege, not a right, and used with discretion. An employee's personal use access rights may be revoked at any time at the discretion of the employee's manager should use be deemed to be excessive or interfering with the employee's performance of their duties.

4.2. Email Guidelines

Certain email content may expose employees and CRAICCHS to legal liability. This includes material that may be construed as sexual harassment, workplace harassment (bullying), defamation, breach of confidentiality and / or copyright infringement.

The following guidelines apply to all employees:

- When engaging in online communication, employees are expected to uphold the values, obligations and expectations of employees outlined in the *Code of Conduct*;
- Any personal use of email must comply with workplace policies, including, (but not limited to) sexual harassment, discrimination and bullying;
- Email is not considered a secure form of communication and the Systems Administrator can potentially view email during the normal course of their work. When deciding what information is to be included in an email, consideration should be given to the fact that it may be forwarded to another party without your knowledge;
- Employees must NOT send or store emails that contain or attach inappropriate, harassing, obscene, racist or offensive material (whether in text, visual or audio form). If any message of an unacceptable nature is received, the recipient should not delete the message, but should notify the General Manager, who will take appropriate action;
- Email is not to be used for storing or distributing information or material that contains anything that may cause or constitute sexual/racial harassment, bullying, or disparagement of others based on their race, national origin, marital status, sex, sexual orientation, age, disability, religious or political beliefs;
- Any personal use of email must not be for on-line gambling purposes or for accessing or transmitting pornography;
- Employees must not transmit CRAICCHS information to their personal email accounts or use a private email account as an alternative to their CRAICCHS email account for sending or receiving any CRAICCHS official communication relating to business activities;

- Broadcasting unsolicited views on social, political, religious, or other non-business-related matters is prohibited;
- Employees must not use email for unauthorised purposes, including sending unauthorised broadcast emails to a group of individuals;
- Employees must **not** send, forward and / or reply to material that may be considered spam, chain letters, phishing, 'junk mail', for-profit messages or hoax emails. If the email appears to be spam, delete without opening any attachments or clicking on any links, which can cause viruses. If in doubt, an employee must contact the General Manager before opening, who may refer it to the Systems Administrator;
- Do not open unexpected email even from people known to you as this might have been spread by a virus;
- Do not run programs directly from websites. If files are downloaded, check for viruses first
- Employees must not personally subscribe to any non-work related external mailing lists or bulletin boards;
- Employees must not send / receive photos or videos without the written explicit approval of their Manager;
- Web based email services are not to be used (i.e. Hotmail);
- Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be maintained in a user's mail box. Messages for archive should be kept in separate archive files stored on the user's network home or shared drive;
- Documents and information that are considered as confidential information to CRAICCHS must not be sent outside the organisation at any time via email;
- Emails and attachments should be kept and filed in accordance with normal administrative practice;
- All incoming messages and attachments will be scanned for computer viruses to ensure the CRAICCHS information technology system is not disabled or corrupted;
- Any virus infections must be reported as a matter of urgency to the General Manager or delegate via voice as soon as practicable, who will contact the Systems Administrator.

4.3. Email Etiquette

- Employees using email should take care in the language they use in drafting email messages. Users should endeavour to be polite, courteous and professional in all messages and to avoid making statements on subjects about which they are uncertain and use common sense to dictate what is acceptable and what is not. Messages that are sent in haste without proper consideration or checking can cause upset, concern or misunderstanding.
- Email should **not** be considered as a secure medium to send private or confidential messages, and as such all information sent over email should be written on the assumption that it may become public knowledge;
- Punctuation and spelling standards should be maintained as if sending a letter;
- Email messages must include a CRAICCHS standard signature at the end of each message;
- Receipt of emails should be regularly checked;
- If unable to answer the email immediately, receipt of the email should be acknowledged with an indication as to when you will be able to respond (as you would for a telephone message);
- Judgement should be used when forwarding emails that you have received to ensure you are not breaching the confidence of the sender or of CRAICCHS.

5. Social Media

Social media are a group of online applications which are designed to allow information to be created, shared, discussed and disseminated. Social media include the sites, tools, channels and platforms used to publish user-generated content and promote social connections and conversations.

This Social Media Policy outlines protocols for using social media to undertake official CRAICCHS business and provides guidance for employees in their personal use of social media. Social media can have a significant impact on the workplace. Social forums such as Facebook and Twitter have blurred the line about what is acceptable conduct in a private forum that can also be viewed publicly. This policy aims to inform CRAICCHS employees how to use social media effectively and appropriately, within CRAICCHS guidelines.

The CRAICCHS policy guiding acceptable use of social media has two parts covering:

1. Business Use - access and use in the workplace; and
2. Private Use - employee responsibilities regarding use of Social Media for their own purposes e.g. Facebook, Instagram and Twitter pages.

Business and personal use of social media by CRAICCHS employees and affiliates must not:

- Bring CRAICCHS into disrepute;
- Compromise the effectiveness of CRAICCHS;
- Defame individuals or organisations;
- Imply CRAICCHS endorsement of personal views; or
- Disclose, without authorisation, confidential information.

5.1. Business Use – Sites / Forums and Authorised Use

All usage of CRAICCHS related social media must be authorised by the General Manager.

Use of and participation in interactive services by employees must reflect and uphold the values, integrity and reputation of CRAICCHS and must comply with the following standards for use;

- Employees have responsibilities under the CRAICCHS *Code of Conduct* which apply when using social media, either personally or for business use.
- Only those authorised to do so by their Manager should undertake social media activity on behalf of CRAICCHS. This includes responding to any comments posted. All social media activity must adhere to all CRAICCHS policies and procedures.
- CRAICCHS will not provide any confidential or proprietary information on social media. All posts and comments will protect and respect privacy and personal information.
- Posts and comments by authorised CRAICCHS staff will always reflect organisational values and culture.
- CRAICCHS must not make reference to clients, colleagues or suppliers without their prior approval.
- CRAICCHS employees must not use social media as a vehicle for the employee's personal views.
- Prohibited communications include; postings that may be considered threatening, discriminatory or harassing spam or junk type postings, profanity or pornography.
- CRAICCHS will ensure that information published is correct and accurate and will cite sources where appropriate.
- CRAICCHS will consider intellectual property and respect copyright. CRAICCHS will always seek permission to use words, images or materials online that the organisation does not own.
- Employees authorised by CRAICCHS to undertake social media activity must review all content before it is posted and consider the impact the activities could have on the individual or the organisation. Employees will use common sense and best judgement. If an employee is in doubt, then the General Manager must be consulted.

5.2. Private Use – Responsibilities as an Employee when using Social Media

Employees should not use their CRAICCHS email address when creating or accessing social networking accounts and should not use CRAICCHS logos that may give the impression of official support or endorsement of personal comments made online.

Statements and/or comments that are published by a CRAICCHS employee via social media (e.g on their personal Facebook and Twitter pages) can be considered to be a public statement. Comments concerning the employees work, the organisation, its employees or clients must abide by the Policies and Procedures of CRAICCHS and must comply with its standards.

CRAICCHS employees using social media for private use (including posting anonymously or using an alias/pseudonym) must uphold the CRAICCHS values and *Code of Conduct* at all times, behaving in a way that upholds the integrity and good reputation of the organisation.

CRAICCHS employees must not use personal social media accounts for business communications.

CRAICCHS employees must not publish or post any comments/allegations/images against the company, clients and employees, that are or could be perceived to be:

- Breaches of workplace confidentiality (even partial disclosures of confidential information);
- Examples of bullying, discrimination and/or harassment, obscene, threatening, hateful to or about work colleagues/peers/the organisation;
- Fraudulent or libellous claims;
- Denigrate the workplace and its employees or the reputation of CRAICCHS;
- Damaging the employee's ability to work with their colleagues;
- Portrayed as representing the organisation's view;
- In breach of CRAICCHS policies and procedures;

Any such activity or breaches of this policy will be considered to be unacceptable behaviour and may be subject to disciplinary action, up to and including termination of an employee's employment in appropriate circumstances.

Any personal social media communication on matters that relate to CRAICCHS should include a personal disclaimer and not the official view of the organisation.

CRAICCHS actively encourages staff to share its posts with their social media networks.

5.3. Use of Social Media for Private Purposes via CRAICCHS server

CRAICCHS permits reasonable personal use of social media provided that this use is lawful, abides by the CRAICCHS *Code of Conduct* and does not:

- Interfere with the performance of the employee's work duties or the duties of others;
- Interfere with the delivery of services to CRAICCHS clients;
- Breach any CRAICCHS policy or procedure;
- Interfere with the operation of CRAICCHS or compromise the reputation or public image of CRAICCHS; or
- Put at risk the integrity of CRAICCHS system; e.g check your account and privacy settings, carefully consider any friend requests– especially from people not personally known.

5.4. Reporting Inappropriate Use of Social Media

If any employee becomes aware of any negative comment made about the organisation, its brand, products or services, or employees on any social media they will not respond directly but inform the General Manager as soon as possible.

CRAICCHS will instigate the relevant investigation, grievance and discipline action as appropriate.

6. Unauthorised Email and Information Technology Use

Any material that is received by email or saved in the CRAICCHS information technology environment which is illegal, discriminatory, racially vilifying or which could reasonably be viewed as inappropriate or offensive or which, in the opinion of CRAICCHS, could reasonably injure the reputation of CRAICCHS must be forwarded to the General Manager for archiving in case of need for future legal reference and deleted immediately. Such material must not, under any circumstances, be forwarded or distributed within or outside CRAICCHS. Storage or distribution of such material will result in disciplinary action, which may include termination of employment.

7. Software

CRAICCHS requires that employees and volunteers use software in compliance with licence terms and conditions.

In order to assist with the prevention and introduction of virus contamination into the software system, computer programs/software not supplied by CRAICCHS must not be downloaded or installed without approval from the System Administrator.

The installation of any copyrighted software for which CRAICCHS does not have an active license is prohibited. (Refer to *Human Resource Management Policy #2.18 Copyright and Intellectual Property, Section 4 Software Licensing and Copyright*).

Installation of privately purchased and owned software on CRAICCHS ICT systems is not allowed without prior approval from the General Manager or Systems Administrator. Proof of purchase is required, consisting of the license certificate and original media, and the invoice if it is available.

8. Ownership

CRAICCHS is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through CRAICCHS ICT systems.

Electronic communications created, sent or received by the users referred to in this Policy are the property of CRAICCHS, and may be accessed as records of evidence in the case of an investigation. Electronic communications may also be subject to discovery in litigation and criminal investigations. Please note that email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications can be held liable for messages that have been sent.

9. Monitoring

Whilst CRAICCHS respects the privacy of users of the ICT systems, CRAICCHS consider any and all data created, stored or transmitted on the ICT system as work material and, as such, expressly reserves the right of authorised persons to monitor and review any data or records on the CRAICCHS ICT system on an intermittent basis without notice to the user. This may include for operational, maintenance, compliance, auditing, security or investigative purposes. For example, electronic communications and websites visited may be monitored.

Use of the CRAICCHS ICT systems constitutes consent to monitoring in accordance with this Policy.

As a user of the CRAICCHS ICT system, employees agree to the following guidelines, including but not limited to:

- Electronic communications and attachments stored on CRAICCHS equipment, whether for CRAICCHS or personal use, may be viewed by CRAICCHS authorised management;
- All email, internet and facsimile transactions and other communications will be monitored and/or intercepted by authorised CRAICCHS personnel and will be referred to relevant law enforcement agencies if appropriate;
- All messages, both incoming and outgoing, will become the property of CRAICCHS, and as such are subject to examination by the General Manager, or any other authorised person, at any time;
- The monitoring and retrieval of email messages may be undertaken in any circumstances where the General Manager believes it is appropriate to do so. These circumstances include, but are not limited to, the following:
    - In the course of an investigation regarding misconduct, discrimination or sexual harassment;
    - To comply with CRAICCHS Workplace Health and Safety obligations;
    - To protect and prevent interference with CRAICCHS business;
    - To locate substantive information required for organisational business, which is not more readily available by some other means.

Disciplinary action may be taken against any employee who use CRAICCHS ICT systems and assets in a manner which breaches policies. Inappropriate use of the CRAICCHS ICT system or breaches of computer policies will be fully investigated and may be grounds for dismissal. CRAICCHS may investigate a complaint arising from the use of the CRAICCHS ICT systems.

If at any time there is reasonable belief that CRAICCHS ICT systems/resources are being used in breach of this Policy, the General Manager/manager of the person who is suspected of using CRAICCHS ICT systems inappropriately may suspend a person's use of CRAICCHS ICT systems/resources and may require that the equipment being used by the person be secured by the General Manager while the suspected breach is being investigated.

10. Complaints

If an employee suspects that this Policy may have been breached, or if they are exposed to an email or other electronic communication (including mobile phone messages), which offends them and / or which they believe is inappropriate, they should contact their manager or the General Manager.

11. Internet Use Education

Staff will be educated and trained in best practice processes when using the internet. This includes learning about protection measures against viruses and spyware. This training will be incorporated into staff induction processes and ongoing through staff meetings, memo's etc.

COPYRIGHT AND INTELLECTUAL PROPERTY

Policy #4.3

Version: June 2018	**Date of Board Approval:**
Last Review Date:	**Next Review Date:** June 2019

Relevant Documents:

- Position Description
- Contract of Employment
- Asset Register
- HR D011 V1 – Staff Code of Conduct
- CG D001 V1 – Board Code of Conduct

PURPOSE

The purpose of this policy is to clarify the status of material subject to copyright used by the organisation, and to remove any possible misunderstandings about ownership of copyright.

POLICY STATEMENT

CRAICCHS aims to conduct its business activities in a manner that is compliant with the provisions of the *Copyright Act 1968* and other copyright licence agreements currently in force. CRAICCHS respects copyright law, the rights of copyright holders and the obligations of content users under Australian Copyright Law. CRAICCHS encourages and supports the legal use of third party copyright content, either in digital, electronic or print format to enhance its business activities.

SCOPE

This policy has direct application for all operations and at all levels within the organisation including the Board of Directors, General Manager, Managers/Supervisors and employees/contractors.

DEFINITIONS

Third party copyright: Third party works are those that have not been created by CRAICCHS and include artwork, logos, images, photographs, diagrams, graphs, tables, text, published articles, music etc.

PROCEDURES

1. Production of Copyright Material

Under law, original material created by CRAICCHS employees in the course of their employment, irrespective of whether it is created using CRAICCHS materials or resources, or during normal working hours, will be owned by CRAICCHS. The meaning of "course of employment" will be determined by the employee's *Position Description* and usual duties. Copyright ownership will be in accordance with the terms stipulated in an employee's *Contract of Employment*.

If any material was created using CRAICCHS resources, or during paid working hours, then the onus is on the employee to demonstrate that it was not created in the course of their employment.

Works by independent contractors shall be owned in accordance with the written contract under which the work was created. CRAICCHS shall ensure that there is a written contract for work by an independent contractor specifying ownership. At law, unless a written contract specifies otherwise, then independent contractors will own copyright in everything that they create.

2. Copyright Notice

Employees of CRAICCHS should ensure that every publication of CRAICCHS, including any books, newsletters, brochures, forms, reports and computer software contains the following statement:

> © [Name of Organisation], Australia, [Year of creation of material]

This statement should not be included in normal business letters, invoices, receipts.

3. Use of Copyright Material

Employees of CRAICCHS are required to observe all applicable copyright laws and regulations.

Employees of CRAICCHS may use copyright material belonging to or licensed to CRAICCHS only for the purposes of their work for CRAICCHS. Where the material is used by CRAICCHS under licence, employees must act in accordance with that licence.

The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be reproduced, published, distributed or adapted by CRAICCHS employees in the course of their work for CRAICCHS without specific authorisation to do so from the copyright owner. Staff may not download or reproduce text, photographs or illustrations found on the internet without authorisation from the copyright owner. This includes for use in external newsletters, reports or presentations. All non-generic images and illustration should be sourced from and with the consent of the creator. Generic images may be obtained from a stock image supplier (e.g. Shutterstock or iStockphoto).

When reproducing or otherwise using third party copyright material, it cannot be assumed that just because something is on the internet that it is free for everybody to copy and use. This includes images on Facebook or photo sharing websites such as Flickr. Acknowledgement of source of the material does not overcome the need for authorisation; actual authorisation is still required.

The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or CRAICCHS liability, despite the belief that the use of such material was permitted.

CRAICCHS supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement. Disciplinary action may be taken by CRAICCHS against an employee engaging in reckless or deliberate copyright infringement, which may include instant dismissal or termination of employment. This is also a breach of the CRAICCHS *Code of Conduct*. Infringement of copyright may also be a criminal offence, with CRAICCHS reporting any such unlawful activity to the relevant authorities.

4. Software Licensing and Copyright

Unauthorised copying of software is illegal under the *Copyright Act 1968* and is strictly forbidden by all CRAICCHS employees. Use of illegal copies of software is also illegal and is also strictly forbidden on any CRAICCHS ICT systems.

Only legitimately acquired software may be used and only in accordance with all applicable licence conditions. CRAICCHS will hold a valid software licence for all software installed on any equipment on the CRAICCHS ICT system.

As part of the *Asset Register*, CRAICCHS will record all software licences and assets to enable verification of software compliance and record all software licences. Software assets may include: application programs, operating system, communications software, including all clinical management software, as well as email, firewall, backup, virus checking and other utilities. Information recorded may include:

- Software name;
- Serial number;
- Date of purchase;
- Renewal dates if applicable;

Original software media and manuals should be stored securely.

The following information will be recorded by the Systems Administrator:

- Software product code and activation key;
- Number of licences purchased;
- Location of software (i.e. serial number of computer where software is installed).

PRIVACY POLICY

Policy #4.4

PRIVACY STATEMENT

CRAICCHS regularly collects and uses individuals' personal information to ensure delivery of appropriate, timely and quality health and wellbeing services. We are committed to ensuring the privacy and confidentiality of all personal information (which includes sensitive and health information). CRAICCHS must comply with the Australian Privacy Principles (APPs) under the Privacy Act 1988, the Information Privacy Act 2009 and other privacy laws that govern how an individual's personal information is handled. CRAICCHS will take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.

SCOPE

This Privacy Policy applies to personal information collected by CRAICCHS, who are governed by the Australian Privacy Principles under the Privacy Act 1988 (Cth) and the Information Privacy Act 2009 (Qld).

CRAICCHS will regularly review this policy to ensure it is in accordance with any changes that may occur. The most up to date copy can be obtained either from our website or by contacting CRAICCHS.

CLIENT CONSENT

When a person registers as a client of CRAICCHS, they provide consent for our General Practitioners and/or staff to collect and use their personal information, so they can provide the best possible healthcare and services to the client. Only staff who need to see a person's personal information will have access to it. If CRAICCHS needs to use a client's information for anything else, additional consent will be sought from the client to do this.

PERSONAL INFORMATION WE COLLECT AND WHY WE COLLECT IT

CRAICCHS collects personal information for a purpose that relates directly to our functions and activities and related business activities.

Clients

CRAICCHS main purpose for collecting, using, holding and sharing a client's personal information is to manage their health and/or to plan, coordinate and provide healthcare or wellbeing services to them. We also use it for directly related business activities, such as financial claims and payments, meeting our reporting accountabilities, upholding our duty of care, practice audits and accreditation, and business processes (e.g. staff training). **CRAICCHS collects and stores your personal information ONLY when it is related to our work with you.**

Clinic Clients:

CRAICCHS collects personal information in order to provide health services. The information CRAICCHS will usually collect about a client includes names, date of birth, addresses, contact details, medical information including health status information, medical history, medications, allergies, adverse events, immunisations, social history, results of clinical investigations and tests, family history and risk factors, Medicare number (where available) for identification and claiming purposes, Healthcare identifiers and health fund details. The information we collect and hold depends on individual circumstances and may include images and recordings.
A client has the right to deal with us anonymously or under a pseudonym unless it is impracticable for CRAICCHS to do so or unless we are required or authorised by law to only deal with identified individuals. If a client provides incomplete or inaccurate information to us or withholds personal health information from us we may not be able to provide the client with the service they are seeking.

Clients of Family Wellbeing Program:

Personal information we collect, use and store may include personal details (name, date of birth, next of kin, address, phone number, gender, languages spoken, identified special needs); names and address of friends/family who may be supportive; significant health, income or other information which may be needed by yourself or CRAICCHS; forms, assessments and work notes (case plans, goals, receipts); information that may be important to you for legal reasons (e.g. disclosure of an assault or crime against you); information that you may request CRAICCHS safeguards on file such as official documents, birth certificates etc. The information we collect and hold depends on individual circumstances.

We are committed to providing you with the highest level of care to support you and your family. We understand that you may not want to provide some information to us. The information we ask of you is relevant to providing you with services you have requested. If you choose not to provide us with some or all of that information we ask, we may not be able to provide you with and services you require.

Employees

Personal information is collected for the primary purpose of processing their entitlements, including payment of wages, superannuation and taxation obligations. Additional information may be collected to protect client and organisational interests. Information held by CRAICCHS may include personal address and contact details, employment history, qualifications, resume, bank account details, superannuation fund membership details, tax file number, police check history, immunisation information, driver license details, workers compensation history and training records.

HOW PERSONAL INFORMATION IS COLLECTED

Information is collected in a number of ways, including:

- Directly from you in most circumstances (such as via registration or other forms, during medical consultations and services, during assessments, completing a survey or feedback form, and from emails or telephone calls);
- From other sources such as another family member, guardian or responsible person, other involved healthcare providers, such as specialists, allied health professionals, hospitals, a health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

We will only collect personal information from other sources if you have consented for us to collect your information in this way or where it is not reasonable or practical for us to collect this information directly from you, or we are required by law to collect information from a third party. This may include where the clients' health may be at risk and personal information is needed to provide them with emergency medical treatment.

HOW PERSONAL INFORMATION IS USED

CRAICCHS only uses personal information for the purpose for which it was collected or for any other purpose that is directly related to our function and activity, however CRAICCHS sometimes shares an individual's personal information:

- With third parties who work with our organisation for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with the Australian Privacy Principles and this policy;
- Where CRAICCHS is authorised to provide an agency (such as the Department of Health) with personal information to enable services to be delivered to a person;
- With other healthcare providers in providing the best care and services to a client;

- When it is required or authorised by law (eg court subpoenas);
- When it is necessary to lessen or prevent a serious threat to a client's life, health or safety or public health or safety, or it is impractical to obtain the client's consent;
- When there is a legal requirement to share certain personal information (e.g. some diseases require mandatory notification);
- During the course of providing medical services, through My Health Record.

Only people who need to access personal information will be able to do so. Other than in the course of providing medical or wellbeing services or as otherwise described in this policy, we will not share personal information with any third party without your consent.

Notwithstanding the above, you have the right to withdraw consent to release your personal information (e.g. for direct marketing) at any time. This can be arranged by contacting CRAICCHS at any time.

CRAICCHS will not share personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without client consent.

STORING AND PROTECTING PERSONAL INFORMATION

Personal information may be stored at our premises in various forms such as paper or electronic records and visual records such as X-rays, CT scans, videos and photos.

CRAICCHS will take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. CRAICCHS uses technologies and processes such as access control procedures (password protection and controlled staff access), network firewalls, encryption and controlling access to health record storage areas to protect privacy. All staff are required to sign confidentiality agreements.

ACCESSING AND CORRECTING PERSONAL INFORMATION

You have the right to request access to, and correction of, personal information held by CRAICCHS by contacting the relevant Manager. CRAICCHS acknowledges clients may request access to their medical records. This request will be evaluated as per the requirements and conditions of privacy legislation.

There may be instances where access is denied to certain records or parts of records as allowed under privacy legislation. Generally, if requested, an individual will be granted access to any personal held about them, however CRAICCHS may deny access to personal information if:

- We believe that it would unreasonably impact the privacy of another individual;
- It may threaten the life, health or safety of another or the public;
- It is unlawful to provide the information;
- The request is vexatious or frivolous.

If we deny access to personal information, we will provide reasons in writing for the decision and provide a process for lodging a complaint.

CRAICCHS will respond within a reasonable timeframe of up to 30 days. A small fee may be charged to meet the costs of extracting and photocopying the information. All requests will require proof of identity or authority, which will be recorded along with the information request.

CRAICCHS will take reasonable steps to make sure personal information we collect, use and disclose is accurate, complete and up to date. From time to time, staff may ask you to verify personal information held by us is correct and current. You may also request, in writing, to the appropriate Manager that CRAICCHS correct or update information. All requests will require proof of identity or authority. If CRAICCHS and the individual cannot agree as to whether the information is accurate, complete, relevant or up-to-date, we will, on request, record a statement of the dispute.

DIRECT MARKETING

From time to time, we may contact you to provide you with information about other services offered by us that may be of benefit to you and your family. This includes information or services that can help improve your wellbeing. We may also provide you with newsletter or other publications. When we contact you, it may be via mail, phone, email or text-message. When you become a client of CRAICCHS you consent to us using your personal information for direct marketing (as described in this document), unless you have contacted us to withdraw your consent. If you do not wish to receive marketing material from us, you can contact us at any time to let us know

COMPLAINTS HANDLING

CRAICCHS take complaints and concerns regarding privacy seriously. If you have any concerns, complaints or suggestions about the management of your personal information we ask that you contact us directly at the details below. CRAICCHS will attempt to resolve the complaint according to our complaint resolution procedure and respond within 30 days. If you are not satisfied with the response, you may contact the Office of the Australian Information Commissioner (OAIC) in writing using the online form www.oaic.gov.au or call 1300 363 992.

CONTACT US

General Manager
CRAICCHS
PO Box 398
Murgon QLD 4605
Ph. (07) 4169 8600

POLICY REVIEW STATEMENT

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. The most up-to-date copy can be obtained by contacting CRAICCHS using the above-mentioned details.

PRIVACY MANAGEMENT

Policy #4.5

Version: June 2018	**Date of Board Approval:**
Last Review Date:	**Next Review Date:** June 2019

References:

- Information Management Systems Policy *#4.1 Computer Information Security*
- Information Management Systems Policy *#4.4 Privacy*
- Human Resources Management Policy *#2.3 Staff Induction*
- Clinic Policy *#6.4 Medical Records Administration Systems*
- Clinic Policy *#7.3 Informed Consent*
- Clinic Policy *#8.1.4 Patient Feedback*
- Family Wellbeing Policy *#6.6 Complaints and Feedback*

Relevant Documents:

- Privacy Collection Statement
- HR D011 V1 - Staff Code of Conduct
- HR D009 V1 - Confidentiality Agreement
- Registration and Consent Form

PURPOSE

The Privacy Act 1988 (Cth) sets out 13 Australian Privacy Principles which set out standards, rights and obligations in relation to collecting, storing, providing access to, using and disclosing personal information. This policy outlines the processes for dealing with personal information in accordance with privacy legislation (including the Information Privacy Act 2009 (Qld)).

POLICY STATEMENT

CRAICCHS respects the privacy of all individuals and believe any personal information collected by us or provided to us should be safely and securely held and used only for the purposes intended and agreed. CRAICCHS will use all reasonable efforts to protect the privacy of individuals' personal information and to comply with the obligations imposed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) and the Information Privacy Act 2009. CRAICCHS supports responsible and transparent handling of personal information.

SCOPE

The scope of this policy has application for all programs, services and staff, general practitioners, contractors, and health professionals involved with the collection, storage, use and disclosure of personal information.

DEFINITIONS

As defined by the Privacy Act 1988:

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not;

Examples include: an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

Personal information can be held in any media, such as paper and in electronic records, X-rays, CT scans, videos, photos and audio recordings. Personal information may be collected by a General Practitioner directly from the client or from a third party in the course of providing a healthcare service.

Health information means:

- Information or an opinion, that is also personal information, about:
  - The health or a disability (at any time) of an individual, or
  - An individual's expressed wishes about future healthcare/services to him/her, or
  - A health service provided, or to be provided, to an individual, or
- Other personal information collected to provide, or in providing, a health service, or
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- Genetic information about an individual.

Health information is regarded as one of the most sensitive types of personal information.

Examples include: information about an individual's physical or mental health, notes of an individual's symptoms or diagnoses and the treatment given, appointment and billing details, prescriptions and an individual's healthcare identifier when it is collected to provide a health service.

Sensitive information (a subset of personal information) means:

- Information or an opinion (that is also personal information) about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association/union, sexual orientation or practices or criminal record;
- Health information about an individual;
- Genetic information (that is not otherwise health information);
- Biometric information.

CRAICCHS ***holds*** personal/health information if they have possession or control of the relevant medical record. This includes reports or other health information from another health organisation such as medical specialists or another health provider.

RESPONSIBILITY

CRAICCHS has designated roles for managing computer and information security and for privacy management. CRAICCHS will provide appropriate education and training to these staff members to ensure an appropriate level of knowledge. These roles may be outsourced to ensure appropriate technical knowledge applicable to the role's responsibilities. This is outlined in our *Information Management Systems Policy #4.1 Computer Information Security.*

All staff, contractors, general practitioners and allied health professionals are responsible for maintaining the confidentiality and privacy of personal information and to respect an individual's right to privacy. Staff commit to this through their signing and acknowledgement of the *Staff Code of Conduct*.

Privacy Officer

CRAICCHS has a designated Privacy Officer (each Program Manager/Coordinator) who implements and monitors adherence to all applicable privacy legislation relevant to CRAICCHS.

The role includes:

- Acting as a liaison for all privacy issues and client requests for access to their personal health information;
- Handling all queries concerning privacy legislation from staff members;
- Ensuring compliance with the Australian Privacy Principles and other legislation
- Developing (in conjunction with the General Manager) and maintaining written policies and procedures for privacy management;
- Liaising with the person responsible for computer and information security and systems.

PROCEDURE

1. Open and Transparent Management of Personal Information

CRAICCHS will manage all personal information held by the organisation in an open and transparent way and will take all reasonable steps to ensure practices, procedures and systems comply with the APPs and other relevant privacy legislation. CRAICCHS has implemented a process to deal with inquiries or complaints from individuals about compliance with the APPs (refer to *Information Management Systems Policy #4.4 Privacy, Section 8 Complaints Handling*).

CRAICCHS will maintain a clearly expressed and up to date Privacy Policy about the management of personal information (refer to *Information Management Systems Policy #4.4 Privacy)*. CRAICCHS will ensure that this policy is readily available free of charge and in an easy to read and appropriate format. The policy will be available to the public:

- On the CRAICCHS website;
- Via a printout on request to our reception staff;
- Displayed in our waiting room so that it can be seen by members of the public.

CRAICCHS will ensure that, upon request, all reasonable steps will be taken to provide a person or body with a copy of the Privacy Policy in the particular form requested.

1.1. Practices, Procedures and Systems Implemented to Ensure APP Compliance

CRAICCHS have implemented the following practices, procedures and systems to assist with complying with the APPs:

- A process for identifying and managing privacy risks over the lifecycle of information (refer to *Information Management Systems Policy #4.1 Computer Information Security*, *Section 4 Risk Assessments of Information Security Risks*);
- Security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure including IT systems, internal access controls and audit trails (refer to *Section 9 Security of Personal Information*);

- Procedures for identifying and responding to privacy breaches, handling access and correction requests (refer to *Section 10 Access to Personal Information*) and receiving and responding to complaints and inquiries (refer to Clinic Policy *#8.1.4 Patient Feedback* and *Family Wellbeing Policy #6.5 Complaints and Feedback*);
- During new client registration procedures, individuals are informed they have the option of not identifying themselves or using a pseudonym and are advised of the consequences of doing this. All new clients are provided with a *Privacy Collection Statement*, and this is also included in the *Privacy Policy* available for all clients;
- CRAICCHS has designated staff members (Program Managers/Coordinator) whose role is to ensure compliance with the privacy legislation:
- All staff are informed about handling personal information and privacy compliance under the APPs as part of our induction program (refer to *Human Resources Management Policy #2.3 Staff Induction*). When updates or changes occur to the APPs or the systems, procedures or practices of CRAICCHS regarding handling personal information, staff are informed through training sessions and information bulletins;
- Staff who regularly handle personal information receive appropriate supervision by the Clinic Manager or Program Manager/Coordinator, with reinforcement of CRAICCHS systems and processes to ensure compliance;
- All staff are required to sign a *Confidentiality Agreement* upon commencing their role with CRAICCHS, affirming their commitment to maintaining privacy and confidentiality.

2. Collection of Personal Information

2.1. Collection of Solicited Personal Information

CRAICCHS collects personal information from individuals and third parties (such as guardians and other health professionals involved in client care) during the provision of healthcare services. CRAICCHS will not collect personal information including health information (other than sensitive information) unless the information is reasonably necessary for the delivery of healthcare services.

CRAICCHS will not collect sensitive information (refer to *Definitions* above) about an individual unless:

- The individual consents to the collection of the information; and
- The information is reasonably necessary for one or more functions or activities; or
- The collection of the information is required or authorised under law or a court order; or
- A permitted general situation exists in relation to the collection of the information https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-c-permitted-general-situations ; or
- A permitted health situation exists in relation to the collection of the information https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-d-permitted-health-situations .

Personal information must be collected in a way which is lawful and fair, without being unreasonably intrusive or using methods of intimidation. CRAICCHS will collect personal information directly from the individual rather than from a third party unless:

- The individual has given consent to CRAICCHS to collect the information from a third party; or
- CRAICCHS is required under law to collect the information from a third party; or
- It is unreasonable or impracticable to collect the personal information directly from the individual.

2.2. Dealing with Unsolicited Personal Information

Unsolicited information is information received without asking. If unsolicited personal information is received, and such information is not reasonably necessary or directly related to CRAICCHS functions or activities and CRAICCHS could not have collected the information, the information will be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so. This does not apply if the unsolicited personal information is contained in a Commonwealth record.

3. Notification of the Collection of Personal Information (Collection Statement)

Clients need to be made aware of the potential use and disclosure of their personal/health information. This will occur for new clients but is not necessary during recurring consultations.

At or before the time of personal or health information collection (or as soon as practicable after), CRAICCHS will take reasonable steps, through provision of a *Privacy Collection Statement*, to inform the person of:

- The full name and address of CRAICCHS;
- The fact and circumstances of collection if personal information is collected from someone other than the individual or the individual may not be aware of the collection;
- Whether the collection is required or authorised by law;
- The purpose for which the information is collected;
- Any consequence (if any) for the individual if all or some of the personal information is not collected;
- Any third parties to which CRAICCHS may disclose the individual's personal information and whether any such party is located overseas;
- A link to CRAICCHS *Privacy Policy* for further information about how the individual may access personal information, seek correction of personal information and complaint about a breach of privacy legislation.

CRAICCHS will inform clients about the collection of personal information through the *Privacy Collection Statement* and via:

- A sign at reception;
- Brochure/s in the waiting area;
- Our client information sheet;
- New client forms;
- Verbally, if appropriate;
- CRAICCHS website.

Obtaining a client's informed consent to the collection, use and sharing of personal information will be a guiding principle for CRAICCHS and should be provided at an early stage in the process of clinical care. To provide informed consent, clients must have sufficient information about their own healthcare and the ability to then make appropriate decisions (refer to *Clinic Policy # 7.3 Informed Consent*).

4. Use or Disclosure of Personal Information

4.1. Use or Disclosure Circumstances

CRAICCHS will only use or disclose personal information it holds for the purpose for which it was collected ('primary purpose'), which is, to provide healthcare or wellbeing services.

Personal/health information may be used or disclosed for another (secondary) purpose where:

- The individual has given consent;
- The individual would reasonably expect CRAICCHS to use or disclose their personal information for the secondary purpose related to their healthcare;
- The information is required or authorised under Australian law (see Section 4.3.1);
- A permitted general situation exists https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-c-permitted-general-situations
- A permitted health situation exists https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-d-permitted-health-situations
- The secondary use is necessary for the enforcement of the law (see Section 4.3).

In the clinic setting, clients will generally expect their health information to be used for a wide variety of activities directly related to the healthcare services they receive, including:

- Providing information about treatments;
- Being treated by a person other than their treating GP, such as a specialist or during admission to hospital;
- Internal assessment practices, such as to assess the feasibility of particular treatments;
- Management, funding, complaint-handling, planning, evaluation and accreditation activities;
- Disclosure to experts or lawyers (for legal opinions), insurers or medical defence organisations to report adverse incidents or for the defence of legal proceedings;
- Disclosure to clinical supervisors.

It is important that CRAICCHS tell individuals what could be done with their personal health information and if it is within the reasonable expectation of the client then personal health information may be disclosed. Where there is doubt as to the client expectations relating to the use or disclosure of the information, consent should be sought. Doctors may need to discuss such requests with the client and perhaps their medical defence organisation.

4.2. Consent

In obtaining consent to the use or disclosure of personal health information, CRAICCHS will ensure:

- The individual is adequately informed before giving consent;
- The individual gives consent voluntarily;
- The consent is current and specific; and
- The individual has the capacity to understand and communicate their consent.

Individuals will be made aware of the *Privacy Collection Statement* when giving consent to share personal information. Prior to an individual signing consent to the use or disclosure of their personal information, they are made aware they can request a full copy of our *Privacy Policy* and *Privacy Collection Statement*.

CRAICCHS will only use or disclose personal information to a third party once the *Registration and Consent Form* is signed on the first visit, and in specific cases, informed consent has been sought. Once signed, the form is scanned into the client's record and is kept on file for future use.

4.3. Third Party Disclosures of Personal Information for a Secondary Purpose

Where health information must be disclosed to a third party, CRAICCHS must consider what information is relevant for the proposed purpose. Clients will reasonably expect the disclosure of only the necessary subset of their health information, along with third-party restrictions. Prior to disclosing any health information, CRAICCHS should carefully examine its authority for disclosure and seek advice where necessary.

As a general rule, no client information is to be released to a third party unless the request is made in writing and provides evidence of a signed authority to release the requested information, to either the client directly or a third party. Where possible, de-identified information is disclosed.

Written requests should be noted in the client's record and also documented in the *Request Register*, which records all requests for access to health information including transfers to other medical practitioners. Requests should be forwarded to the designated person within the clinic for follow-up.

Requested records are to be reviewed by the treating medical practitioner or principal doctor prior to their release to a third party. Where a report or medical record is documented for release to a third party, having satisfied criteria for release, (including the clients written consent and where appropriate written authorisation from the treating doctor), then the practice may specify a charge to be incurred by the client or third party, to meet the cost of time spent preparing the report or photocopying the record.

Where hard copy medical records are sent to third parties, copies are to be forwarded not original documentation, where possible. If originals are required, copies are to me made in case of loss.

Security of any health information requested must be maintained when transferring requested records and electronic data transmission of client health information from the clinic must be in a secure format.

4.3.1. Court Order, Subpoenas and Disclosure Required by Law

CRAICCHs are legally required or authorised to disclose health information in certain circumstances, including for mandatory reporting purposes (e.g. regarding communicable diseases or suspected child abuse). CRAICCHS may also receive demands for medical files as part of legal proceedings (e.g. where a client is suing the General Practitioner, or another organisation and medical records are relevant). Requests for third party access to personal/health information should be initiated by either receipt of correspondence from a government agency, court or a solicitor (subpoena or discovery order). CRAICCHS may seek legal advice where necessary in relation to subpoenas or discovery orders.

In such circumstances, a note is to be made in the medical record of the date the request was received and if applicable the date of the court case.

4.3.2. Enforcement Body (Police, Customs, Crime Commission etc)

Before sharing personal information to an enforcement body, CRAICCHS must have a reasonable basis for belief that the use or disclosure is reasonably necessary. CRAICCHs must be able to justify its belief. This may be, for example, in response to a written request by an enforcement body (signed and dated by an authorised person). At other times this basis may be less clear and CRAICCHS will need to reflect more carefully about whether it is reasonable. CRAICCHS should ensure it only uses or discloses the minimum amount of personal/health information reasonably necessary.

CRAICCHS must make a written note in the *Request Register* of this use or disclosure including the following details:

- The date of the use or disclosure;
- Details of the personal information that was used or disclosed;
- The enforcement body conducting the enforcement related activity;
- If CRAICCHS used or disclosed the personal information, how the personal information was used and to whom it was disclosed;
- The basis for CRAICCHS's reasonable belief.

4.3.3. Other Third-Party Disclosures

In the case of the following third-party requests, the query should be directed to the client's medical practitioner:

- External doctors and health care institutions;
- Health insurance companies, workers compensation, Social Welfare Agencies;
- Government agencies such as Medicare, Department of Veterans Affairs, Centrelink (may refer to a medical defence organisation).

4.3.4. Accounts / Debt Collection

CRAICCHS must maintain privacy of client's financial accounts. Accounts are not stored or left visible in areas where members of the public have unrestricted access.

Accounts must not contain any clinical information. Invoices and statements should be reviewed prior to forwarding to third parties such as insurance companies or debt collection agencies.

Outstanding account queries or disputes should be directed to the practice manager/bookkeeper or principal.

4.3.5. Researchers / Quality Assurance Programs

Where CRAICCHS seeks to participate in human research activities and/or continuous quality improvement (CQI) activities, client anonymity will be protected. CRAICCHS will also seek and retain a copy of client consent to any specific data collection for research purposes.

Research requests are to be approved by the General Manager and must have approval from a Human Research Ethics Committee (HREC) constituted under the NH&MRC guidelines. A copy of this approval will be retained by CRAICCHS.

Practice accreditation is a recognised peer review process and the reviewing of medical records for accreditation purposes has been deemed as a "secondary purpose" by the Office of the Australian Information Commissioner. As a consequence, clients are not required to provide consent.

4.3.6. Disease Registers

CRAICCHS submits client data to various disease specific registers (cervical, breast bowel screening etc) to assist with preventative health management.

Consent is required from the client with the option of opting in or opting out. Clients are advised of this via a sign in the waiting area and in the clinic's information leaflet.

5. Direct Marketing

Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.

CRAICCHS will only use or disclose personal information (not including sensitive information) about an individual for direct marketing if the individual would reasonably expect CRAICCHS to use information for that purpose, a simple 'opt-out' mechanism is available for individuals to request not to receive direct marketing and the individual has not made such a request. The 'opt-out' mechanism will be included in the *Registration and Consent Form* which is completed by all new clients.

An individual may request at any time not to receive direct marketing communications from CRAICCHS by writing to the organisation.

6. Cross Border Disclosure of Personal Information

CRAICCHS does not disclose any personal information overseas through any data management or transmission platform.

7. Adoption, Use or Disclosure of Government Related Identifiers

An *identifier* is a number, letter or symbol, or a combination of any or all of these things, that is used to identify the individual or to verify the identity of the individual.

A *government related identifier* is an identifier that has been assigned by a government or agency (such as Medicare numbers, Centrelink Reference numbers, driver licence numbers, Australian passport numbers).

CRAICCHS will not adopt a government related identifier of an individual as its own identifier of the individual unless it is required or authorised by law.

CRAICCHS must not use or disclose a government related identifier of an individual, unless:

- It is reasonably necessary for CRAICCHS to verify the identity of the individual for the purpose of CRAICCHS business; or
- It is reasonably necessary for CRAICCHS to fulfil its to a government agency; or
- It is required or authorised by law; or
- CRAICCHS reasonably believes it is necessary for the enforcement of the law; or
- A permitted general situation exists (refer to Section 2)

8. Quality of Personal Information

CRAICCHS will take reasonable steps to ensure that personal information it collects is accurate, up to date and complete.

CRAICCHS will also take reasonable steps to ensure that the personal information used or disclosed is, having regard to the purpose for the use or disclosure, accurate, up to date, complete and relevant.

Regular reviews of the quality of personal information held by CRAICCHS will assist in ensuring it is accurate, up to date, complete and relevant.

Reasonable steps taken by CRAICCHS include:

- Implementing internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information, including training staff in these systems and procedures;
- Implementing protocols that ensure personal information is collected and recorded in a consistent format. Notes will also be recorded on when the personal information was collected and the point in time to which it relates, and if it is an opinion;
- Ensuring updated or new personal information is promptly added to relevant existing records;
- From time to time, staff will ask a client to verify personal information held by our organisation is correct and current;

- Reminding individuals to update their personal information each time clinic staff engages with the individual;

9. Security of Personal Information

CRAICCHS will take reasonable steps to protect personal information held from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Reasonable steps taken by CRAICCHS include implementing strategies in relation to the following:

- Governance, culture and training;
- Internal practices, procedures and systems (refer to *Information Management Systems Policy #4.1 Computer Information Security*, *Section 1.1 Practices, Procedures and Systems Implemented to Ensure APP Compliance*);
- ICT security (refer to *Information Management Systems Policy #4.1 Computer Information Security*);
- Access security (refer to *Information Management Systems Policy #4.1 Computer Information Security*);
- Third party providers, including cloud computing (refer to *Information Management Systems Policy #4.1 Computer Information Security, Section 11 Cloud Computing*);
- Data breaches protocols (refer to *Information Management Systems Policy #4.1 Computer Information Security, Section 5 Data Breach Response and Recording*);
- Physical security;
- Destruction or de-identification of personal information;
- Relevant standards and guidance on information security.

These strategies are outlined in *Information Management Systems Policy #4.1 Computer Information Security.*

9.1. Governance Culture and Training

CRAICCHS privacy and security governance arrangements include appropriate training, resourcing and management focus to foster a privacy and security aware culture among staff (refer to *Information Management Systems Policy #4.1 Computer Information Security, Section 2 Developing a Security Culture).* Governance arrangements in relation to personal information include risk management strategies and business continuity plans (refer to *Information Management Systems Policy #4.1 Computer Information Security*, *Section 4 Risk Assessments of Information Security Risks* and *Section 9 Business Continuity and Information Recovery*).

CRAICCHS has established clear procedures for oversight, accountability and lines of authority for decisions regarding personal information security. Each Program Manager is responsible for personal information held, where and how it is held and responsible for ensuring that it is held securely.

Staff are aware of the importance of good information handling and privacy and security practices. Privacy training with staff will ensure they understand their responsibilities and avoid practices that would breach CRAICCHS's privacy obligations.

9.2. Physical Security

Physical security at CRAICCHS is an important part of ensuring that personal information is not inappropriately accessed.

Physical measures for protecting the security of personal information include:

- Filing cabinets which hold personal information are locked, with only authorised staff having key access;
- Building security alarm systems to detect unauthorised access to the building;
- An access monitoring system to detect unauthorised or after-hours access to the building;

- Workstations positions so that computer screens cannot be easily read by unauthorised third parties;
- Visitor access is controlled, with unauthorised areas for clients or visitors;

For information stored electronically, security measures include:

- Password protection;
- Automatic computer log offs;
- Log file/electronic audit trails;
- Fire walls, malware and virus protection
- Data encryption.

Refer to *Information Management Systems Policy #4.1 Computer Information Security.*

9.3. Destroying or De-identifying Personal Information

Where CRAICCHS no longer needs personal information for any purpose for which the information may be used or disclosed, reasonable steps will be taken to destroy the information or ensure it is de-identified, except where:

- The personal information is part of a Commonwealth record; and
- CRAICCHS is required by or under Australian law to retain the personal information.

The Clinic Manager is responsible for identifying personal information that is required to be retained by law or under a Commonwealth record (refer to *Clinic Policy # 6.4, Medical Records Administration Systems*)

Where personal information needs to be destroyed or de-identified, CRAICCHS will take reasonable steps to destroy or de-identify all copies it holds of the personal information, including copies that have been archived or are held back as back-ups.

Reasonable steps taken by CRAICCHS include:

- Personal information held in hard copy will be destroyed through a process of shredding prior to disposal;
- Where personal information held is held in electronic copy, the hardware will be 'sanitised' to completely remove stored personal information;
- Personal information stored by a third party such as cloud storage will require verification from the third party that secure destruction of this information has occurred;
- The Network Administrator will ensure that back-ups of personal information are also destroyed or 'put beyond use'.

The Clinic Manager is responsible for the destruction of personal information and is informed of document destruction procedures.

10. Access to Personal Information

10.1. Scope of Access

Clients of CRAICCHS have the right to access their personal information (including medical records) under the privacy legislation, subject to limited exceptions. Where CRAICCHS holds personal information about an individual, we will, on request, give the individual access to that information according to privacy legislation. A client's medical record includes all information created by the treating medical practitioner/s or received from other practitioners, and usually exists in both electronic and hard copy documents. This will affect information held on CRAICCHS's administrative system and in the medical record.

A client's right to access their personal information is explained to each client through the *Privacy Policy, Privacy Collection Statement* and is explained to each client. A notice is displayed in the waiting room and on the organisations web site advising clients and others of their rights of access and of CRAICCHS commitment to privacy legislation compliance. An information brochure is also available that provides further details if required.

10.2. Procedure for Accessing Personal Information

10.2.1. Request Received

When a client requests access to their medical record and related personal information held at this clinic, each request is documented and CRAICCHS will endeavour to assist clients in granting access where possible and according to the privacy legislation. Exemptions to access will be noted and each client or legally nominated representative will have their identification checked prior to access being granted.

A client may make a request verbally at the clinic, via telephone or in writing to the Program Manager e.g. fax, email or letter. No reason is required to be given. The request is referred to the client's doctor or delegated Privacy Officer.

A form is completed to ensure correct processing. Once completed the form filed/scanned in the client record.

Verifying an Individual's Identity

CRAICCHS must be satisfied that the request has been made by the individual concerned or by another person who is authorised to make a request on their behalf (e.g. a legal guardian). The steps appropriate to verify an individual's identity will depend on the circumstances, such as whether the individual is already known to CRAICCHS, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure.

The identity of the requesting individual should be confirmed through sighting of personal identification in a face-to-face meeting (such as a driver's licence, passport or proof of identity card) or through over the telephone through requesting information that can be checked against records held by CRAICCHS. CRAICCHS will record that an identity document was sighted, or identity verified on the *Request for Personal Health Information* form.

Request by Another Person (Not Client)

An individual may authorise a responsible person to be given access to their personal information, if they have the right, such as a legal guardian, and if they have a signed authority (e.g. power of attorney). Under 'APP6 Use or Disclosure of Personal Information', CRAICCHS may disclose health information to a 'responsible person' for an individual. This is permitted where the client is:

- Physically or legally incapable of giving or communicating consent;
- Disclosing information is not contrary to the wishes of the client;
- The disclosure is necessary to provide appropriate care or treatment of the client or for compassionate reasons.

Identity validation as outlined above.

The Privacy Act 1998 defines a 'responsible person' as a parent of the individual, a child or sibling of the individual who is at least 18 years old, a spouse or de facto spouse, a relative (at least 18 years old and a member of the household), a guardian or a person exercising an enduring power of attorney granted by the individual that can be exercised for that person's health, a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency

Children and Young People

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. CRAICCHS will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for CRAICCHS to assess the capacity of individuals under the age of 18 on a case-by-case basis, CRAICCHS may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

10.3. Acknowledge Request

Each request is to be acknowledged with a letter sent to the client (within 14 days or sooner if possible) confirming the request has been received and notifying the individual and/or their legal representative of the anticipated length of time required before their personal information can be made available and any charges involved in processing the request.

CRAICCHs must respond within a reasonable period after the request to access personal information is made. CRAICCHS will aim to respond within 30 calendar days, however this depends on the scope and clarity of the request, whether the information can be readily located and assembled, and whether the consultation with the individual or other parties is required.

10.4. Fees Charged

Upon receiving the request to access personal information, CRAICCHS will discuss with the individual what information they wish to access, and the expected fees involved.

Giving access to personal information may incur costs to CRAICCHS for retrieval from archive storage or administrative costs (e.g. photocopying). Should this be the case, a fee may be charged for the provision of information, however the fee will not be excessive. Where access fees are to be applied, the individual will be informed as soon as possible after submitting the request for access, such as in the acknowledgement letter.

10.5. Collate and Assess Information

CRAICCHS will retrieve the client's hardcopy medical record or arrange for the treating medical practitioner with the Clinic Manager to access the computer record.

Appropriate staff will be trained in the process to correctly identify clients using 3 patient identifiers, name, date of birth, address or gender to ascertain we have the correct client record before actioning or releasing anything from that record.

CRAICCHS may refuse access to personal information as outlined in Section 10.6. The General Manager is responsible for reviewing the contents of any requested personal information and ensuring that any content falling within exemption provisions as outlined in *Section 10.6* is deleted or access is provided in an alternative format (see *Section 10.7*).

10.6. Refusing to Give Access to Personal Information

Under the APP's, CRAICCHS is not required to give an individual access to personal information on the following grounds:

- CRAICCHS reasonably believes giving access to that information would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- Giving access would have an unreasonable impact on the privacy of other individuals; or
- The request for access is frivolous or vexatious; or
- The information relates to existing or anticipated legal proceedings between CRAICCHS and the individual, and would not be accessible by the process of discovery in those proceedings; or
- Giving access would reveal the intentions of CRAICCHS in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- CRAICCHS has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to CRAICCHS functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- Giving access would reveal evaluative information generated within CRAICCHS in connection with a commercially sensitive decision-making process.

10.7. Provide Access

CRAICCHS must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so. This may be, for example by:

- Obtaining a copy by email, fax, in person, hard copy or an electronic record or over the phone;
- View and inspect the information with the possibility of talking the contents through with the General Practitioner;
- Listening to an audio tape or viewing a video.

Factors CRAICCHS will consider when assessing what manner to provide the information include the volume of information requested, the nature of the information requested, and any special needs of the individual requesting the information.

Prior to granting access to the personal information, identity of the individual must be verified and noted on the appropriate form. CRAICCHS must also verify that the person has authority to gain access to the personal information (check age, legal guardian documents, authorised representative etc.). Refer to Section 10.2.1.

If a client is viewing their personal information, supervision needs to be provided to ensure the client is not disturbed and no information goes missing.

If a copy is to be given to the client, CRAICCHS must ensure that all pages are checked prior to providing them to a client, with a note made on the request form.

If a General Practitioner is to explain the contents to a client, ensure that an appointment time is made for the client.

10.8. Providing Access in an Alternative Way

Where CRAICCHS refuses to give access to personal information (refer to *Section 10.5*) or refuses to give access in the way requested by the individual, CRAICCHS will try to give access in an alternative way that meets the needs of CRAICCHS and the individual. This will be done through consulting with the individual to try and satisfy their request. The following alternative means of access may be considered:

- Deleting any personal information where there are grounds for refusing access and giving the redacted version to the individual (i.e. this may be by using a black felt tip marking pen to cross out the exempt or irrelevant information);
- Giving a summary of the requested personal information to the individual;
- Giving access to the requested personal information in an alternative format;
- Allowing an inspection of a hard copy of the requested personal information and permitting the individual to take notes;
- Organising access to the requested personal information through a mutually agreed intermediary.

If CRAICCHS refuses to give access, or to give access in the manner requested by the individual, CRAICCHS must give the individual written information which sets out the reasons for the refusal (except where listing the reason for refusal would be unreasonable to do so), and the way in which the individual may complain about the refusal, both internally and externally. A record must be made on the *Request for Personal Health Information* form.

10.9. Access by Employees to Employee Records

The handling of an employees' personal information by CRAICCHS (as a private sector employer) is exempt from the Privacy Act if it is directly related to:

- An employee's current or former relationship;
- An employee record relating to the employee.

This means that CRAICCHS does not need to comply with the APP's when it handles current and past employee records for something that is directly related to the employment relationship and does not have to grant an employee access to their employee records under the Privacy Act.

11. Correction of Personal Information

CRAICCHS will take reasonable steps to correct personal information held to ensure that it is accurate, up to date, complete, relevant and not misleading, having regard to the purpose for which it is held. This applies to where CRAICCHS believes the information is incorrect, out of date, incomplete, irrelevant or misleading or where an individual requests CRAICCHS to correct their personal information.

Where CRAICCHS believes that personal information it holds may be incorrect, CRAICCHS will endeavour to confirm that the information is incorrect before correcting it. Where there is a disagreement about whether the information is indeed correct, CRAICCHS will attach a statement to the original record outlining the clients' claims.

CRAICCHS will endeavour to determine that the request to correct personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf (e.g. a legal guardian).

CRAICCHS will respond within a reasonable timeframe (preferably within 30 calendar days) after the request to correct personal information is made.

CRAICCHS will respond by correcting the personal information as requested by the individual, or by notifying the individual of its refusal to correct it.

Any corrections made to personal information are attached to the original health record.

12. Privacy Review and Monitoring

CRAICCHS will ensure that a program is in place of proactive reviews and audits of the adequacy and currency of the organisations Privacy Policy, and of the practices, procedures and systems implemented under the APP's. This will occur systematically through scheduled privacy audits as well as in the event of any issues or complaints relating to privacy matters.

In conducting an audit, the Privacy Officer is to review the following:

- Review of CRAICCHS Privacy Policy to ensure it reflects the organisation's information handling practices;
- The primary purpose of the organisation;
- What data is collected and documented;
- How this information is stored and who has access;
- What data is disclosed and to whom;
- When and how client consent is obtained;

The Privacy Officer will review the following information and documents:

- Information is collected from hard copy and electronic storage devices and issues discussed with General Practitioners and staff to gain the most current information and practices;
- National and state privacy laws are referenced, with any updates being noted and actioned;
- The *Information Management Systems Policy # 4.4 Privacy* and *Policy #4.5 Privacy Management*, privacy forms and *Access Register*, along with any brochures/client privacy information are to be reviewed and updated if required;
- Review requirements for any of the above client information to be provided in another language or format to ensure client access in a clear and easy to read free format;

COMMUNICATION AND MEDIA

Policy #4.6

Version: June 2018	**Date of Board Approval:**
Last Review Date:	**Next Review Date:** June 2019

References:

- Information Management Systems Policy *#4.2 Acceptable Use of Information and Communication Technology Systems*
- Information Management Systems Policy *#4.3 Copyright and Intellectual Property*
- Information Management Systems Policy *#4.4 Privacy*
- Information Management Systems Policy *#4.5 Privacy Management*
- Human Resource Management Policy *#2.4 Performance Review, Development and Training*
- Human Resources Management Policy *#2.7 Code of Conduct*
- Corporate Governance Policy *#1.7 Board Code of Conduct*

Relevant Documents:

- HR D011 V1 – Staff Code of Conduct
- HR D038 V1 – Employee Feedback Form
- HR D039 V1 - Staff Satisfaction Survey
- CG D001 V1 – Board Code of Conduct
- Media Consent Form
- CRAICCHS Organisational Chart
- CRAICCHS Constitution

PURPOSE

CRAICCHS is committed to effective distribution and receipt of information and communication within the organisation and with clients, stakeholders, and the media. CRAICCHS values good communication and believes it is a critical element of creating a successful, safe and efficient organisation. The purpose of this policy is to provide guidance to CRAICCHS in developing and implementing communication strategies through the various channels.

POLICY STATEMENT

CRAICCHS will establish open and respectful channels of communication with staff, clients and stakeholders to ensure that information distributed is relevant, easy to access, accurate and appropriate in both content and quality. CRAICCHS will continue to develop communication tools to improve information sharing and collaboration between staff, in line with legislative requirements and standards of best practice.

SCOPE

This policy applies to the Board of Directors and all employees of CRAICCHS.

DEFINITIONS

External communication is an exchange of information which occurs between the organisation and external parties, such as clients and community members;

Internal communication is an exchange of information and knowledge which occurs within the organisation.

PRINCIPLES

This policy is based on the following principles:

- Communication systems and equipment will be used only for the purpose of achieving the organisation's objectives;
- Clear, consistent and equitable communication within the organisation is essential for effective operations;
- All communications are presented in plain English language, with language that is simple and easy to understand;
- External communication, including with the media, aligns with the organisation's strategic objectives;
- All communication must adhere to all privacy legislation and the *Information Management Systems Policy #4.5 Privacy Management;*
- All information technology and communications facilities must be used sensibly, lawfully and consistently with an employee's duties as outlined in the *Information Management Systems Policy #4.2 Acceptable Use of Information and Communication Technology Systems;*
- CRAICCHS will, to the best of its knowledge, ensure that all information distributed is accurate, consistent and timely.

RESPONSIBILITIES

Board of Directors

The Board of Directors has primary accountability for keeping key stakeholders informed of strategic directions, operational plans and organisational performance. Communication to the media on matters associated with CRAICCHS is the responsibility of the Chairperson of the Board of Directors.

General Manager

The General Manager has delegated operational responsibility for all internal communications to employees and to create an open communication culture that distributes the relevant information to all stakeholders.

The General Manager will not ordinarily make any public comment except where the Board has given its authority to do so.

Managers/Supervisors

Managers and supervisors are responsible for working with the General Manager to facilitate internal communication flows to employees.

Managers and supervisors will ensure that all employees under their supervision are informed of any changes to policy or procedures which will impact on them.

Employees

Employees have a responsibility to communicate in a professional manner at all times and to observe all communication restrictions and privacy and confidentiality responsibilities.

Employees have a responsibility to read and understand all information that is communicated to them. They are to share information as appropriate.

PURPOSE

1. Internal Communication

1.1. Purpose of Internal Communication

Effective internal communication is essential for good organisational management. CRAICCHS will provide open and explanatory information. All Board, staff and volunteers are responsible for actively contributing to communication strategies and activities.

CRAICCHS will communicate internally with staff for several purposes, including to:

- Make sure that the organisation's vision, goals, policies and guidelines are communicated and strive to give employees the information they need to do their jobs effectively, when they need it, in order to increase understanding and commitment, build motivation, and support CRAICCHS strategies;
- Share knowledge internally about CRAICCHS and its development for effective organisational management;
- Provide employees with clear standards and expectations for their work;
- Communicate with employees about decisions and events that affect them before (if possible) and never later than when information is communicated externally;
- Encourage two-way dialogue at all levels and develop possibilities for employees to give feedback and to be part of an open, inclusive communications climate.

Any messages communicated internally should be purposeful, concise, tailored to the audience, timely and consistent.

1.2. Mechanisms and Tools Used for Internal Communication

CRAICCHS recognise that the organisation has a diverse group of employees, differing in working hours, tenure and type of work and is committed to identifying the best methods of communication to suit and reach our diverse team. A range of mechanisms and tools are used for internal communication including, but not limited to:

Staff and Team Meetings

Staff and team meetings provide opportunity for information sharing and decision-making on a range of project and operational issues for the organisation. All staff are required to attend staff meetings and relevant staff attend team meetings as appropriate. Staff are encouraged to actively raise suggestions through these meetings as a way to participate in continuous improvement. Management is responsible for ensuring that all staff under their supervision are informed of any changes in policy or practice which will impact on them.

Board Meetings

Board meetings support effective governance for the organisation. Board meetings may also include time for staff to communicate with the Board on a range of project and operational issues for the organisation.

Email and Electronic Calendars

The use of email and electronic calendars is essential for effective communication amongst staff, volunteers and management. These tools are a simple and effective way to share information about projects, meetings, internal business/operations, external sector news and activity. These tools should be used whenever possible to save time and to provide a written record which is dated and may be considered formal documentation.

Email and internet use by all employees must adhere to the *Information Management Systems Policy #4.2 Acceptable Use of Information and Communication Technology Systems* and the CRAICCHS *Code of Conduct*.

Staff Memorandums / Bulletins / Newsletters / Noticeboard

Distribution of information from CRAICCHS management or the Board to staff which is important and relevant to their interests, including training, employment vacancies, announcements and policy changes will be communicated via the most appropriate method.

Information received from external sources such as professional journals, research reports, guidelines, training opportunities and conferences will be distributed to all relevant employees by the most appropriate method.

Staff Surveys

A *Staff Satisfaction Survey* will be distributed annually to employees to evaluate their satisfaction with their work environment. This forms part of the continuous quality improvement processes at CRAICCHS. Refer to *Human Resource Management Policy #2.4 Performance Review, Development and Training, Section 5.2 Staff Feedback*.

Staff Feedback

CRAICCHS encourages employees to provide comments or suggestions to improve services, processes and procedures by completing an *Employee Feedback Form.* Refer to *Human Resource Management Policy #2.4 Performance Review, Development and Training, Section 5.2 Staff Feedback.*

Regular, Directed Conversations With / Between Staff

Management are to make genuine efforts to create an atmosphere of trust and good, open communication with staff. An open-door policy is to be practiced by all management team members. Staff are to be encouraged to approach their relevant supervisor/manager whenever they have an issue or query about the application of policies and procedures, work practices or any other issue.

2. External Communication

2.1. Responsibility

The Board of Directors has primary accountability for keeping key stakeholders informed of strategic directions, operational plans and organisational performance.

2.2. Purpose of External Communication

CRAICCHS will communicate externally with key stakeholders for several purposes, including to:

- Increase awareness of the organisation, its vision, goals and purpose, its work, and its needs with a view to supporting organisational strategic direction and decisions;
- Enhance community understanding of its target group, services and broader primary health care issues;
- Promote information about CRAICCHS's operations, especially achievements;
- Share knowledge with its stakeholders.

The key stakeholders for CRAICCHS to communicate with include:

- Funding organisations and their Ministers, including Queensland Health and the Commonwealth Departments of Health and Social Services;

- Partner organisations for project, policy, client support and other activities (including hospitals and health services and private sector companies);
- Peak bodies – state and national (including QAIHC)
- Primary health care and community sector organisations (including CQ RAICCHO);
- Legal and regulatory bodies, particularly ASIC and the Australian Taxation Office;
- Other Government departments and branches including federal, state and local;
- Clients and potential clients;
- Members of CRAICCHS, through the Chairperson;
- Media.

2.3. Developing External Communications

CRAICCHS will conceptualise and develop effective communications structured around the following:

- **What**: Identify broadly what it is that is to be communicated;
- **Message**: Use a message to communicate;
- **Audience**: Identify who the audience is and adapt the message accordingly;
- **Messenger**: Identify who will do the communicating and why;
- **Mechanism**: How will the message be communicated;
- **Review**: Was the message received, understood, did it create interest, was there any feedback.

2.4. Mechanisms and Tools Used for External Communication

The communication options the Board can authorise include:

- CRAICCHS website, incorporating news stories/newsletter;
- General meetings of members;
- Annual Reports and Financial Statements;
- Media releases;

A range of mechanisms and tools are to be used to distribute external communication including, but not limited to:

2.4.1. Website

The website is to be used as a primary electronic marketing tool for distributing outgoing information to a broad audience, to promote the organisation goals and purpose and strategic direction, to build corporate credibility and to promote our services, programs and events.

The Board of Directors is responsible for ensuring:

- Authorisation and registration of the domain name;
- Decisions on the design of the CRAICCHS website including uploaded images, content, menus accessible, banners, logos and website links;
- Content is updated as required;
- Contracting an external website administrator to be responsible for hosting, supporting and maintaining functional applications and administration of the website.

The website content will include:

- Information about the organisation's vision, goals and purpose, structure and background;
- Services provided;
- Governance and the Board;
- Membership;
- Activities, current projects and latest news including media releases;
- How to contact the organisation;
- Complaints and feedback process
- The Privacy Policy.

2.4.2. General Meetings of Members

General meetings will be called and held in accordance with the *CRAICCHS Constitution* and used as a means for the Board of Directors to communicate with Members of the organisation.

2.4.3. Organisational Documents (including Annual Report/Financial Statements)

CRAICCHS produces a number of organisation and project specific documents that provide information about its plans, achievements and activities. Documents such as annual reports, strategic plans, client brochures and project background and implementation plans may be provided to clients, members, stakeholders and funders, with current information about CRAICCHS activities, performance and plans.

The Board of Directors are responsible for authorising organisational policy and planning documents.

Organisational documents for outgoing communication are also to be distributed internally, to all staff and Board of Directors members.

2.4.4. Newsletter

The newsletter is produced monthly with a primary target audience of clients, staff, members of the organisation and members in the community. The General Manager is responsible for approving the content for the newsletter.

2.4.5. Correspondence

CRAICCHS corresponds with a variety of external stakeholders including clients, community members, organisations and government departments.

CRAICCHS's written correspondence is a formal record of the organisation and requires appropriate authorisation before being issued.

Letters should be printed on the correct letterhead and be proof-read prior to sending to ensure accuracy.

A record will be maintained of all incoming and outgoing business correspondence, registered in an electronic mail register, which records date, recipient, any special delivery arrangements such as express, registered etc. Emails sent externally remain a formal record of CRAICCHS and must abide by the *Information Management Systems Policy #4.2 Acceptable Use of Information and Communication Technology Systems.*

3. Media Communications, Marketing and Promotions

3.1. Objectives and Values

CRAICCHS goals in working with the media is to:

- Advocate for the vision, goals and purpose of the organisation;
- Promote the brand, image and work of the organisation;
- Inform the public of the details of the organisation;
- Assist in fundraising for the organisation.

It will be a goal of CRAICCHS to establish and maintain a strong and open relationship with the local media to enable the organisation to communicate important public information and messages about its work and goals in a strategic, timely and positive manner.

CRAICCHS will operate on the values of:

- **Honesty:** The organisation will never knowingly mislead the public, media or staff on an issue or news story;
- **Transparency:** The organisation will promote openness and accessibility in our dealings with the media, whilst complying with the law and maintaining confidentiality when appropriate;
- **Clarity:** All communications with the media will be written in plain English, simple and easy to understand;
- **Balance:** Information provided to the media by CRAICCHS will as far as humanly possible be objective, balanced, accurate, informative and timely.

3.2. Official Spokespersons

CRAICCHS has established delegations of authority as to who in the organisation may communicate with the media. The Chairperson of the Board of Directors is authorised to provide public comment on:

- Any speculation concerning Board meetings or the outcomes of Board meetings;
- Annual and half-yearly financial statements, at the time of their adoption by the Board;
- Resolutions to be put to Special and/or Annual General Meetings;
- Changes in Directors, any matter relating to the composition of the Board (e.g. skills-based Directors), or Board processes;
- Changes in the Constitution;
- Service, geographic coverage or client issues;
- CRAICCHS's future outlook/strategic directions;
- Proposed or actual legal action;
- Other matters specifically related to Members of CRAICCHS.

The General Manager will not ordinarily make any public comment except where the Board of Directors has given its authorisation.

If a Director or an employee is approached by the media for public comment, they must:

(a) Refer the person seeking comment to the Chairperson or to the General Manager;

(b) Do not disclose any information, documents or other forms of data to the person seeking comment without the prior consent of the Chairperson;

(c) Inform the Chairperson or General Manager of the name of the person seeking comment, the reason for the contact (both explicit and inferred), as well as a summary of any other relevant information as soon as possible.

It should always be made absolutely clear whether the views put forward regarding any issue relating to CRAICCHS are those of the organisation or an individual. At all times, consideration should be given as to how the correspondence may affect the reputation of CRAICCHS.

All staff are encouraged to identify initiatives that have the potential to generate positive media coverage and to forward those to the General Manager.

3.3. Use of Images and Content

Use of images and content must have the consent of the owner or be an image owned by CRAICCHS, with any content not infringing copyright. Refer to *Information Management Systems Policy #4.3 Copyright and Intellectual Property*. The *Media Consent Form* must be completed and signed by all individuals (or parents/guardians in the case of children) prior to their image or details being used on the website, in publications or in the media.

All media releases for promotion or other activities, programs or events are to be approved by the General Manager prior to use or release. All media releases and promotional materials released by CRAICCHS must be consistent with the values, goals and purpose of the organisation, support our corporate reputation and reflect the CRAICCHS *Human Resources Management Policy #2.7 Code of Conduct* and *Corporate Governance Policy #1.7 Board Code of Conduct*.

The delegated spokesperson for CRAICCHS will exercise discretion when dealing with the media and refrain from comments regarding confidential, operational, client or staff issues and abide by all privacy legislation and the *Information Management Systems Policy #4.5 Privacy Management*. CRAICCHS reserves the right to withhold certain sensitive information concerning commercial transactions or governmental negotiations.

All content included in all communications and publications must abide by the *Information Management Systems Policy #4.2 Acceptable Use of Information and Communication Technology Systems.*

3.4. Marketing and Promotions

CRAICCHS aims to create a visual identity that is recognisable by the community. The promotional and marketing products used by CRAICCHS include business cards, stationery (including letterhead), publications, reports, newsletters and organisational brochures. All of these publications must clearly display the CRAICCHS name, contact details and logo in a consistent manner to gain strong brand recognition in the community.

Electronic communication including email signatures must also follow the above protocols relating to the CRAICCHS name, contact details and logo.

The Board of Directors is responsible for the planning, design and production of any marketing or promotional materials, within the allocated budget. Final designs for any marketing and promotions are to be presented to the Board of Directors for final endorsement.

4. Communication Hierarchy

Through the *CRAICCHS Organisational Chart*, there is a correct line of communication. As outlined on the *CRAICCHS Organisational Chart,* an employee's first line of communication is through their immediate supervisor or manager, where any issue or concern they may have is to be raised. A supervisor or manager may then take an employee's concern to the next level or advise the employee to do so in certain circumstances.

5. Acknowledgement of Funding

CRAICCHS is required to acknowledge the funding received from various government sources in all publications and any promotional materials in line with Service Agreements and Funding Contracts.