INFORMATION TECHNOLOGY POLICY

Source Documents

- QLD *Disability Services Act* (2006)
- QLD *Disability Services Regulations* (2006)
- Human Services Quality Framework
- Information Privacy Act (2009)

Purpose

- To provide guidelines for the access to and usage of all electronic resources of Real Community Services (RCS)

Scope

- All staff and volunteers
- This applies to the use of all RCS equipment such as:
  - Computers, laptops and tablets
  - Mobile phones
  - Remote Desktop Connections Video or camera, &
  - Any other technical devices that are provided for business purposes

Definitions

User – refers to any person

Virus/Malware **–**a computer program that upsets the operation of computer and/or stored information. Usually imported through the email system, internet sites or through an infected file/drive

Images are described as video (including sound), photos, logos, animations or cartoons (including sound) and any other text, pictorial, or sound representations captured on a camera device

Policy

This Policy has been formulated with the following goals in mind:

- To ensure the security, reliability and privacy of RCS systems, network and data, and that of others.
- To avoid situations that may cause RCS to incur legal liability.
- To encourage the responsible use of network resources, while discouraging practices that degrade the usability of network resources

INFORMATION TECHNOLOGY POLICY

Procedures

Access to technology provides the opportunity to source data from multiple sources. RCS staff and volunteers are encouraged to responsibly utilise the resources that provide this opportunity

Users are prohibited from transmitting on or through any of the RCS services, any material that is or may be considered a civil or criminal offence, or is obscene, threatening or abusive.

1. **The following usage is unauthorised;**

- accessing and using social network sites for example www.facebook.com.au
- To engage in commercial activities for personal gain.
- Users may not access personal emails or messages unless written permission is provided by Management. This includes but is not restricted to sites such as yahoo, msn, hotmail, gmail.
- To engage in any unauthorised fund raising activity, participate in any lobbying activity or engage in any political activity.
- Users may not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material wished to be downloaded or copied.
- Users may not agree to a license or download any material without first obtaining the written permission of the Service Manager or Managing Director.
- Unless expressly authorised to do so, users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to RCS.
- Users are not permitted to access internet services or provide technology resources to clients or non RCS staff and volunteers without the written permission of Service Manager or Managing Director

2. System Access and Network Security

- Users are not to try and log in as someone else, or deliberately try to access known security/confidential files.
- Users are not to provide their log in information to any other users.
- Users may not attempt to interfere with the service to any user, host or network. eg: deliberate attempts to crash or disrupt another system.
- The computer network is the property of the RCS and is to be used for legitimate work purposes, in a professional, lawful and ethical manner.
- If you connect to the RCS network from your home, it must only be authorised by your supervisor at a time that is stipulated (Unless your position duties require otherwise). When connected to the RCS Network, you are still using the RCS's network facilities and this policy must govern your activities and behaviour.

3. RCS Authority

INFORMATION TECHNOLOGY POLICY

- RCS has the right to monitor and log any and all aspects of its computer system including, but not limited to internet tabs, external drives accessed and all communications sent and received by users.
- The RCS has the right to restrict certain file types or access to internet sites that may cause harm to the RCS system or reputation or is not considered as part of a legitimate work function.

4. General Conduct

- Users may use the technology resources for personal use only with written permission from the Service Manager.
- It is the responsibility of users to restrict/monitor internet sites /e-mails that may contravene this policy. Should users gain access to inappropriate sites or receive emails that may contravene this policy, they are to alert management immediately.
- Under no circumstances are users to allow family or friends to access their account.
- Users must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others for example downloading large files during peak hours.
- Files obtained from sources outside RCS may pose a danger and cause damage to RCS computer infrastructure. Users should never download files from the internet or use external drives/disks from non-RCS sources, without first scanning the material with an RCS approved virus checking software. If you suspect that a virus has been introduced onto a computer or RCS network, notify the System Administrator or Managing Director immediately.
- Storing, transmitting, downloading, processing or displaying offensive or obscene material, such as pornography or “hate literature” is expressly forbidden.
- Users are prohibited from downloading or transmitting any obscene image that contains full/partial nudity, or which depicts acts of a sexual nature or acts of a degrading or violent nature
- Do not transmit jokes/material that contains sexual innuendo or obscenity. Material which might foster prejudice or hatred on the grounds of race, gender, sexual orientation or religion is not acceptable and must be immediately and permanently deleted if you happen to receive such material.

Use of Cameras and Other Media

RCS provides a range of resources for users to perform their daily duties. Media that may be used from time to time include;

- Photographic Cameras (Film Type)
- Digital Cameras (Media Card type)
- Video Cameras
- Mobile Telephones

INFORMATION TECHNOLOGY POLICY

In each case, the use of technology should coincide with this policy. Technology resources are provided for legitimate work purposes and must not be used if it;

- Is not directly or specifically work related
- Has not had the appropriate legal written consent of the person/s (or guardian) being photographed
- Is of a pornographic, discriminatory, or harassing nature.

All staff are expressly forbidden to capture any image or sound on their personal devices unless prior permission by the Service Manager has been provided in writing

Monitoring and Investigation

- Management reserves the right to enter, search, and/or monitor RCS technology systems and resources without notice.
- Users learning of any misuse of the technology resources should notify a supervisor immediately.
- Should an investigation be required, passwords and access codes must be made available to management or network administrator upon request.
- RCS has the right to utilize software that makes it possible to identify and block access to data deemed inappropriate

Breach of Policy

Any breach of this policy may expose RCS and you to claims of discrimination, harassment and criminal behaviour.

Failure to follow this policy will result in suspended usage rights and disciplinary action.

If deemed appropriate, police may also be notified.

Evaluation

Review Date:	05 May 2015
Author:	T. Green (Director)
Implemented:	07 May 2015
Review Cycle:	24 Months
Next Review Due:	08 May 2017