The Hut
Community Centre

POLICY	Information & Communication Technology Policy		
DOCUMENT REF	PS ICT 01	EFFECTIVE DATE	11 Feb 2021
RESPONSIBILITY	Board / EO	REVISION NO.	Version 1

Purpose and Scope

This policy aims to ensure the security of The Hut's Information Communication and Technology (ICT) infrastructure, equipment, software and other IT applications provided through providing ICT users guidance in the use of these resources.

Information and Communication Technology (ICT) includes any electronic device or application used to communicate, create, disseminate, store or manage information such as text, images, audio or video.

This policy applies to all Hut staff and workers who have access to The Hut's online information and systems.

Definitions

Staff	Paid employees and volunteers.

Background

Information is an asset that is critical to The Hut's service delivery and operations. Therefore, all information that is captured, stored, processed and delivered by The Hut, regardless of form or format, must be protected proportionate to its value and risk.

The Hut, at various times and when there is a purpose to do so, will collect and store personal and/or confidential information. If not stored correctly, with appropriate security processes and measures in place, access to this information could be obtained or used illegally and subsequent harm could be caused to individuals or to the organisation.

The Hut also depends heavily on the use of social media and its website, in particular for disseminating information about programs and services.

Policy

The Hut is committed to ensuring staff and workers have access to ICT infrastructure, tools, training and support that assists them to do their work efficiently and effectively.

Files will be stored on an external server located in Australia or country where data integrity is equal to or higher than in Australia. Appropriate anti virus software will be installed on all computers with a separate antivirus on cloud drives and storage.

The Hut Community Centre

Access levels to all information and software applications will follow the principle of "need to know", i.e. only the minimum level of access to perform the task or duties is granted. To protect information, a system of controlled permissions, passwords and privileges safeguarding access to the shared drive, files and media platforms will be established and maintained.

All use of social media, the internet, shared drives and The Hut's website will be used in accord with The Hut Code of Conduct and Privacy Policy and screening and training for staff will be undertaken where required.

Public accessible computers will be divorced from The Hut's administration and network system.

Cyber security requirements will be included as part of The Hut's business resilience planning and incorporated into business continuity and service recovery procedures.

Objective

The objective of this Policy and all associated procedures is to provide a framework for appropriate safeguarding measures to be put in place that will ensure The Hut has maximum security in place to protect it from cyber risks and maintain the confidentiality of personal and sensitive information.

Responsibility

The Board is responsible for reviewing this Policy and ensuring all procedures and systems relating to the Board and its sub-committee are adhered to.

The EO is responsible to enact this policy.

Related Documents	ICT – Usage and Security Procedures Privacy Policy Delegation of Authority Hut Code of Conduct
Legislation & References	Copyright Act 1968 Privacy Act 1988

Signed on behalf of Hut Board by Hut Chair:
Name: Loraine F Scheide Signed: _[signature]_   Date: 11/2/2021

Date Approved by Board: February 2021	Next Review Date: February 2024