Section	A8.1.3	**Version**	1	FINAL
Label	Central Office	**Document Type:**	Guidelines	
Responsible	Andrew Lewis	**Created**	30 June 2022	
Author	Paul Cavicchia	**Review Due**	30 June 2024	
File Name				

EMAIL SECURITY/ACCEPTABLE USE POLICY - GUIDELINES

Policies & Procedures

Version	Date	Author	Approved by	Review Due	Summary of Changes
1	08/02/2022	Paul Cavicchia	Andrew Lewis	30/06/2024	Initial Version

Approval

Name	Position	Signature	Date
Andrew Lewis	CEO		20 October 2020

Section	A8.1.3	**Version**	1	FINAL
Label	Central Office	**Document Type:**	Guidelines	
Responsible	Andrew Lewis	**Created**	30 June 2022	
Author	Paul Cavicchia	**Review Due**	30 June 2024	
File Name				

IT Acceptable Use -Guidelines

Purpose

The purpose of these guidelines is to set appropriate acceptable use parameters for the Information Technology systems, to ensure the continued effective and secure operation of those systems and to protect CTI from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

These guidelines should be read in conjunction with the Acceptable Use Policy.

Scope

These guidelines apply to:

- all users
- any use of the systems, whether or not during business hours, on CTI premises or through the use of privately owned devices or facilities

Authorised use

The systems are primarily a CTI tool, to be used for CTI purposes by staff, suppliers, and contractors.

- In the case of staff, this includes uses relevant to their employment with CTI
- In the case of contractors and suppliers, this includes uses for the purpose for which they have been given access to the systems

Personal use

Any personal use of CTI equipment and systems should be incidental and not interfere with the user's role within CTI, the work of others or the operation of the systems.

However, unreasonable or excessive personal use is not permitted. For example, the systems must not be used to conduct a personal business or private commercial activity, gamble, objectionable material or carry out excessive and regular research into topics not related to work or study.

Ownership of data and intellectual property

Subject to CTI's Policies and regulations, CTI is the owner of all data:

- created by employees as part of their employment; and
- created, sent or received by users using the systems,

and all such data may be accessed as records of evidence, including in an investigation or in response to other actions such as audit, litigation or criminal investigations.

The ownership of intellectual property created by staff, contractors and suppliers, visitors and participants in projects is governed by Intellectual Property Regulations:

- *Australian Copyright Act 1968 (Cth)*
- *Intellectual Property Regulations 2017*
- *Patents Act 1990*
- *Patents Regulations 1991*
- *Trade Marks Act 1995 except Part 13 which the Australian Customs Service administers*
- *Trade Marks Regulations 1995*
- *Designs Act 2003 - this came into force on 17 June 2004*
- *Designs Regulations 2004*

Conditions of access

It is a condition of access to the systems that users must agree to comply with all CTI's policies relating to the use of computing facilities, including these guidelines.

Users:

- are presumed to be responsible for all activities undertaken using their accounts
- must take reasonable steps to keep their account secure
- must choose a password that cannot easily be guessed or predicted
- must not share their password with anyone else or record their password in obvious locations
- must change their password regularly (and immediately if it becomes known by another person)
- must not permit other persons to use their account (other than through an email proxy arrangement or unless approved in advance by the RTO Manager
- must log out or lock their computers whenever they are left unattended
- must protect the security of data held on mobile systems (e.g. phones, laptops, memory sticks and other storage mediums), including by maintaining reasonable virus control measures where possible
- must not connect unauthorised devices to the network, either via software or hardware that makes this possible (e.g. attaching a personal computer or external storage device)
- must make sure that important CTI data that is not included in automatic backups is manually backed up on a regular basis and can be recovered to the latest version in the event of data loss
- must not use abusive, profane, threatening, racist, sexist, or otherwise objectionable language in any message
- must not access, send, receive, store, or print pornographic, racist, sexist, or otherwise discriminatory, or objectionable material
- must report actual or suspected security breaches to the IT Service Desk as soon as possible
- must not defeat or attempt to defeat security restrictions on systems and applications
- must not remove or disable antivirus and other similar client security agents without approval from the CEO
- must not use or install unauthorized or unlicensed software
- knowingly propagate or disseminate malicious software of any type

Unauthorised and illegal uses

Users must not use the systems to engage in offensive, unlawful or illegal behaviour.

Email and other electronic communications

Email is an official method of communication for staff. Mass electronic communications are moderated by the Internal Communications team.

Privacy

Users must deal with personal information in accordance with CTI's Privacy Statement.

Access, monitoring, filtering and blocking

Users:

- use the systems on the understanding and condition that their use is monitored
- acknowledge and consent to CTI's right to access, monitor, filter and block electronic communications created, sent or received by any user using the systems

Subject to the approval and at the discretion of the CEO or other authorised person and for compliance with applicable legislation, CTI reserves the right to (without notice):

- intercept, access, monitor and use electronic communications created, sent or received by users of the systems in any manner determined by CTI (including as records of evidence in an investigation or in response to other actions such as audit, litigation, criminal investigations or freedom of information requests)
- monitor the use of any device or terminal
- inspect any data residing on any CTI-owned resource (regardless of data ownership and including personal emails and other personal communications and data stored in personal file directories)
- capture and inspect any data in any computing infrastructure owned by CTI
- delete or modify any data in its network
- re-image its desktops and laptops as and when required
- apply filtering systems to the network that limit use and activity by preventing communications based on size or content

For example, communications may be blocked if they are suspected:

- to contain unlawful material
- to be unsolicited commercial electronic messages within the meaning of the Spam Act 2003 (Cth).
- establish processes to block access to websites deemed inappropriate

For example, CTI may block access to:

- websites deemed to be a security risk
- websites that may cause a negative impact on the systems
- websites that affect network bandwidth detrimentally
- websites deemed to contain offensive or unlawful material
- internet protocols and methods deemed insecure
- websites that contravene CTI's policies in any way
- remove any material deemed to be offensive, indecent or inappropriate (including obscene material, defamatory, fraudulent or deceptive statements, threatening, intimidating or harassing statements, or material that violates the privacy rights or property of others)
- check, filter, block and moderate comments and conversations published through CTI controlled channels and media and remove content that is in breach of applicable laws, codes and policies

CTI also collects utilisation statistics based upon network address, network protocol application use or user-based.

Destruction of CTI data

Users who store CTI data on a privately owned device or facility are responsible for ensuring that CTI's data is rendered illegible and irretrievable at the time of disposal of that device or facility.

Breach of these guidelines

Access to the systems may be suspended or terminated at any time if these guidelines are breached. In addition:

- staff who breach these guidelines will be referred to the CTI Manager and dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (whichever is applicable).
- affiliates who breach these guidelines will be referred to the RTO Manager and dealt with in accordance with the relevant processes

A breach of these guidelines may also be:

- a breach of third-party rights (such as an infringement of intellectual property rights)
- a criminal offence (such as serious acts of harassment, bullying and occupational violence and vilification)

In addition to any disciplinary action by CTI, this may lead to civil or criminal proceedings and penalties, which CTI may report to relevant law enforcement bodies and for which the user will be held personally accountable.

In some exceptional circumstances (for example where access to objectionable material relates directly to a user's employment with CTI), subject to the approval of and at the discretion of authorised persons, an exemption may be granted for activities that would otherwise breach these guidelines. Exemptions may be required to be approved in advance by the CEO.

Complaints

Users who receive an internal or external electronic communication that is offensive or inappropriate, should in the case of staff and affiliates, raise it with their Group Manager (or if the manager is the cause of the complaint with HR or the CEO).