CSIRO Responsible use of ICT and Internet Services

This procedure provides direction on the responsible use of information and communication technology (ICT) and internet services at CSIRO (CSIRO ICT resources).

Contents

Procedure Scope

This procedure applies to all staff and CSIRO affiliates (users). Where this procedure refers to staff or staff members it also applies to CSIRO affiliates.

The purpose of this procedure is to:

- facilitate the appropriate, effective and equitable use of ICT and internet services at CSIRO (CSIRO ICT resources)
- ensure that the use of CSIRO ICT resources is legal, ethical and consistent with the aims, values and objectives of CSIRO.

Context

CSIRO relies heavily upon technology to fulfil its mission of 'solving the greatest challenges using innovative science and technology'.

Defining how that technology is used is critical in ensuring that CSIRO is able to fulfil this mission. It also helps reduce the risk of ICT failures or incidents.

Detailed Procedure

Use of ICT resources

This procedure applies to all users of CSIRO ICT resources. The use of ICT resources includes use of:

- devices, systems, networks, or services
- CSIRO networks and services from personal devices.

You must comply with the following principles of use when using CSIRO ICT resources

Principle	Description
Protect our interests	CSIRO ICT resources shall not be used in a way that could cause the organisation embarrassment or loss, or in the interests other than those of CSIRO.
Lawful use	CSIRO ICT resources shall only be used for lawful activities and cannot be used for any activities which would contravene any laws or regulations with which you or CSIRO are obliged to comply.
Commonwealth first	CSIRO ICT resources shall be used by personnel to perform their duties on behalf of the Commonwealth.
Respect your peers	CSIRO monitors the use of its technology and information. Only use CSIRO technology in a manner that will not cause harm or offence to your peers, especially if it were public knowledge.
If in doubt, ask	If you are not sure about specific access or the use of ICT assets, services and information, or whether you're doing the right thing, ask IMT.
Report issues	If you see something that does not appear right, let IMT know. Security is everyone's responsibility.
Approved use	Only authorised ICT equipment, software, and services shall be introduced and used in the CSIRO environment.

A guide to responsible use

The right to access, use or possess CSIRO's ICT resources comes with obligations and requirements. CSIRO expects that users are responsible for their own actions when using its ICT resources. The following information is provided as a guide for users of CSIRO ICT resources. It is not an exhaustive list of what is, and is not, considered responsible use.

Responsible use of CSIRO ICT resources

You must protect your data and CSIRO's data by:

- having an authorised CSIRO account (IDENT)
- not sharing your CSIRO credentials with anyone
- locking your device or session when away from your ICT device
- keeping your CSIRO ICT resources secure and reporting theft or misplacement
- adhering to the instructions of any CSIRO cyber security awareness communications
- not accessing or attempting to gain access to unauthorised data, files or other information
- keeping all CSIRO data confidential unless the information has been approved for external publication, this includes information provided in confidence to CSIRO by other entities
- not taking CSIRO devices on personal leave overseas unless approved by your line manager
- complying with applicable legislation, including the:
  - Copyright Act 1968
  - Criminal Code Act 1995
  - Cybercrime Act 2001
  - Privacy Act 1988
  - Spam Act 2003
- complying with contractual and license agreements.

Irresponsible use of CSIRO ICT Resources

You must not use CSIRO ICT resources to undertake actions or access content which is offensive or inappropriate, this includes:

- bullying
- pornographic
- harassing
- hateful
- racist
- sexist
- abusive
- obscene
- discriminatory
- defamatory
- offensive
- threatening
- espionage
- excessively violent
- acts of political activism.

You must not use CSIRO ICT resources in a way that is likely to contravene the law

Examples of illegal use and content include:

- child pornography
- intending to form inappropriate relationships, abuse, grooming, exploitation or misusing personal data of persons under the age of 18 years
- acts of terrorism
- defamatory material
- material that constitutes racial or religious vilification
- unlawfully discriminatory material
- stalking
- blackmail
- threats
- breach of copyright laws
- fraudulent activity
- personal gain
- online gambling
- computer crimes and other computer offences under the applicable legislation.

These uses may be a criminal offence and will be referred to police or other relevant authority if appropriate.

You must not use CSIRO ICT resources in a way that adversely impacts CSIRO or its partners' systems, networks, or services

Examples of activities that could adversely impact CSIRO or its partners' systems, networks, or services include:

- allowing unauthorised access to ICT resources
- installing third party software that changes, deactivates or circumvents any existing security controls
- using a VPN without authorisation
- wilfully or maliciously opening or distributing computer viruses
- failing to implement appropriate physical security controls such as locking computers when left unattended
- circumventing or disabling IMT-installed software, services or security measures
- intentionally bypassing security controls or exploiting security deficiencies
- torrenting software (where software is downloaded from multiple sources simultaneously)
- copying CSIRO data from CSIRO ICT assets to non-CSIRO owned physical devices and/or non-CSIRO managed cloud services without authorisation
- failing to abide by the licencing conditions of content, programs, software

- copying or distributing copyrighted materials, software, music or media without express permission of the copyright holder or as otherwise allowed by law
- mining cryptocurrencies.

You must not misuse Commonwealth assets

Examples of misusing Commonwealth assets include:

- breaking Australian laws, legislation and guidelines
- using CSIRO ICT resources in a manner that contradicts the obligations and behaviour expected of staff and affiliates
- using CSIRO ICT resources for personal gain
- giving away or selling CSIRO IT equipment, software, licences or services to third parties unless contractually agreed and approved by an IMT Delegate (Rank 4)
- allowing third parties use CSIRO IT equipment, software, licences or services without contractual agreement or approval by an IMT Delegate (Rank 4).

You must not create any other ICT or cyber security risk, as deemed by the Chief Information Officer or the Chief Information Security Officer

Monitoring use of CSIRO ICT Resources

CSIRO monitors the use of its technology and information. Only use CSIRO technology in a manner which will not cause harm or offence to your peers, especially if it were public knowledge.

If you see something that doesn't appear right, let IMT know. Security is everyone's responsibility.

Use of CSIRO ICT resources is not private. IMT may monitor usage to ensure compliance with applicable laws and CSIRO policy.

In order to safeguard CSIRO ICT resources, IMT implements security controls and may implement additional countermeasures should the misuse of CSIRO ICT resources be discovered. Countermeasures may include:

- removing an ICT resource from the network
- disabling an account
- confiscating devices
- referring a matter to Human Resources, Security and Fraud.

Roles and Responsibilities

Staff and CSIRO affiliates must:

- follow this procedure when they are using ICT resources
- contact IMT with any questions about responsible use of ICT resources
- contact IMT if they see something that doesn't appear right in relation to use of ICT resources.

IMT will:

- provide guidance regarding the responsible use of CSIRO ICT resources
- issue new guidance regarding responsible use, as required
- update this procedure as required to reflect any changes related to the responsible use of CSIRO ICT resources
- review this procedure every two years to ensure accuracy and currency.

Supporting Documents and Links

Code of Conduct

Cyber Security Principles

Privacy Policy

Travel Procedure

Workplace Issues Resolution Procedure

Criminal Code Act 1995

Glossary

ICT resources

IMT

Includes but is not limited to all CSIRO networks, systems, software and hardware including local area networks, wide area networks, wireless networks, intranets, email systems, computer systems, software, servers, desktop computers, printers, scanners, personal computers (desktops, notebooks and tablets), mobile phones, portable storage devices including digital cameras and USB memory sticks, hand held devices, any cloud platform or service that contains CSIRO information or data and other ICT storage devices.

User

A user is any person with an authorised account to access to CSIRO ICT resources.

Accountability

Authors: IMT

Functional areas consulted: IMT

Approver (Rank 6 delegate): Brendan Dalton, Chief Information Officer (CIO)

Date of Final Approval: Version 1.0 approved 10/01/20, Version 1.1 approved 25/07/22

Version: V1.1

Review date: 25/07/24