SHARED SERVICES

ACT Government Acceptable Use Policy

CMTEDD
Chief Ministers, Treasury and Economic Development Directorate

Version 2.6, 08/01/2019

Contents

Introduction

Purpose

The Acceptable Use of ICT Resources Policy ("Acceptable Use Policy") instructs ACT Public Service employees and contractors ("staff") in the acceptable use of information and communications technology (ICT) resources, including:

- Acceptable use
- Prohibited use
- Information security
- Security practices
- Compliance

The policy is issued by agreement of all ACT Government directorates and is published under the auspices of the Shared Services ICT Collaboration Forum.

Background

Staff are provided with ICT resources and services by the ACT Government to perform their duties.

This policy is based on the overarching principle that staff using ICT resources must comply with:

- *Public Sector Management Act 1994* (the PSM Act)
- *Public Sector Management Standards 2006* (the PSM Standards), and
- Public Service Code of Conduct.

Scope

This policy applies to all ICT resources, devices and services including:

- desktop computers and devices
- mobile devices such as laptops, tablets and smartphones provided by ACT Government
- personally-owned devices connected to ACT Government resources and
- network, server, storage and cloud resources.

Reference

- *Public Sector Management Act 1994*
- *Public Sector Management Standards 2006*
- Public Service Code of Conduct
- ACT Protective Security Policy Framework
- ICT Policy Waiver Process
- ICT Security Policy
- *Workplace Privacy Act 2011*
- *Information Privacy Act (ACT) 2014*
- *Health Records (Privacy and Access) Act 1997*
- *Disability Discrimination Act 1992*
- *Sex Discrimination Act 1984*
- *Crimes Act 1914*
- *Criminal Code Act 1995*
- *Copyright Act 1968*
- *Freedom of Information Act 1989*

Directorates may have complementary policies and legislation that must also be complied with.

Contact Officer

For all queries about this policy, staff should contact ICT Security.

Responsibilities

Role	Responsibilities
Supervisors ACTPS employees supervising other staff	Oversee the acceptable use of ICT resources. Act when they become aware of a breach of this policy. Escalate any continuing and ongoing policy breaches. Ensure staff are aware of their responsibilities under this policy and the consequences of inappropriate behaviour. Approve requests for use normally prohibited by Whole-of-Government and directorate policies.
All staff ACTPS employees: permanent, temporary and casual Non-ACTPS staff: contractors, consultants and volunteers	Use ACT Government ICT resources in accordance with this policy. Inform supervisors when they become aware of breaches of this policy by other staff. Report any security incidents to the appropriate channels.
JACS Security & Emergency Management Branch	Responsible for developing whole-of-government policy on public sector protective security.
Agency Security Advisors	Responsible for day-to-day management of the protective security measures within the directorate or agency. Develops, implements and monitors directorate or agency security procedures and systems. Analyses the directorate or agency's security environment and posture, and plans measures to manage security risks.
Agency Security Executives	The delegate of the Director-General or CEO with authority to approve protective security programs for their directorate or agency.
Directors-General and agency heads	Responsible under the PSPF for the security of their information and ICT systems.
Shared Services	Responsible for the security of ACT Government ICT infrastructure and Whole-of-Government ICT systems.
ICT Security	Responsible for developing whole-of-government ICT security policy, standards and strategies. A team comprised of the CISO, ITSMs, security analysts and investigators who provide ICT security advice and implement and operate whole-of-government security measures.
Chief Information Security Officer (CISO)	Also referred to as the **Information Technology Security Advisor (ITSA)**. A Whole-of-Government role that manages the strategic direction of ICT security for ACT Government and the implementation and operation of Whole-of-Government security measures.
Information Technology Security Manager (ITSM)	A delegate of the ITSA responsible for a specialist discipline in ICT security.

Acceptable use

Acceptable use of ACT Government ICT resources is governed by the ACT Public Service Code of Conduct, the ACT Public Sector Management Standards and the *Public Sector Management Act 1994*. You must:

- manage the ICT resources entrusted to you honestly and responsibly
- avoid wasteful or extravagance excessive use of ICT resources, and
- not allow personal use to interfere with your official duties.

Official use

ACT Government ICT resources are the property of the ACT Government and may only be lawfully used in the manner that the ACT Government permits.

You are only permitted to use ICT resources for the performance of your official duties, subject to the Personal Use terms below.

All other use of ICT resources is prohibited without prior written approval.

Access to ICT resources

Use ACT Government ICT resources only for the purpose for you are authorised.

Do not attempt to access any ICT resource including data or programs that you do not have authorisation or explicit consent to access.

Personal use

You may make reasonable personal use of some ACT Government ICT resources, such as email and web browsing on the desktop or laptop computer that is issued to you, or a corporate smartphone or tablet, provided it is not **prohibited use** as defined by this policy.

Do not allow personal correspondence, phone calls, web browsing or other ICT resources to interfere with your official duties or with the work of other staff or facilities required for business purposes.

Consider including a disclaimer in any personal communication making it clear the opinions expressed are your own and do not represent the views of the ACT Government.

Do not access or download large personal files or unapproved software or save them to shared ICT resources such as a network drive.

Use good judgement and seek advice from your supervisor if you are unsure what constitutes reasonable personal use.

Directorates may prohibit certain ICT resources such as business and infrastructure systems from personal use – the exclusions will be explained to you when access to these ICT resources is provided.

Your personal use of ICT resources may be restricted, or other disciplinary action taken if personal use interferes with ACT Government business, operational effectiveness, clients, staff or property.

BYOD

Do not use your own ICT devices for official use without prior written approval from your supervisor. This is called a “bring your own device” (BYOD) arrangement.

Do not use your own ICT devices (e.g. your personal computer, laptop, tablet or smartphone) on ACT Government networks. The exception is the ACT Government TUUD and Public Wi Fi networks, subject their Terms of Use.

You must comply with the Mobile Device Security Policy and the Remote Access Security Policy when accessing official information such as ACT Government email from your own ICT device.

Your personal information

The ACT Government will use personal information about you including your name, position, staff number and business contact details (email, phone, location) to provide ICT services.

When you voluntarily provide other information such as your personal mobile number, email address or home address to the ACT Government, you agree that this information may also be used to provide ICT services.

The provision of ICT services may entail testing, training and support of ICT systems, which may be carried out on premises or in outsourced arrangements with approved service providers.

Prohibited use

Prohibited use of ACT Government ICT resources and information is governed by the Public Sector Management Act 1994, in Section 9(o):

- Do not make improper use of the property of the Territory.

Further detail is provided by the ACT Public Sector Management Standards 2006, in Part 2.4(19):

- Do not access, download or store inappropriate or prohibited material.
- Do not use ICT resources to communicate inappropriate or prohibited material.

Improper activities

Do not create, communicate, access, download or store inappropriate or prohibited material using ACT Government ICT resources unless it is part of your official duty to do so.

Do not use ICT resources to engage in any unlawful conduct, including any conduct that contravenes the *Information Privacy Act (ACT) 2014*, the *Copyright Act 1968*, the *Spam Act 2003*, the *Do Not Call Register Act 2006*, the *Telecommunications Act 1997*, the *Telecommunications (Interception and Access) Act 1979*, the *Archives Act 1983*, the *Sex Discrimination Act 1984*, the *Disability Discrimination Act 1992*, the *Crimes Act 1914*, the *Criminal Code Act 1995*, or the *Public Sector Management Act 1994*.

Do not use ICT resources to engage in any conduct that may make a person feel offended, humiliated and/or intimidated, where that reaction is reasonable in the circumstances (e.g. communicating a suggestive, graphic or sexually explicit message).

Do not use ICT resources to engage in any conduct that vilifies, harasses or discriminated against a person based on their race, sex, sexual preference or identity, religion or disability.

Obtain prior written approval from your supervisor and Shared Services ICT Security if you have an official need to access material that would normally be prohibited under this policy.

Unlawful or improper use of ICT resources may result in suspension of access, disciplinary action or legal proceedings.

Inappropriate or prohibited material

Inappropriate material includes information that could damage the ACT Government’s reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory.

Prohibited material includes pornography and other offensive material. Possession of certain kinds of pornography (such as child pornography) is a crime and Shared Services ICT is required to report such activity to the Australian Federal Police. Material may be pornographic under the *Criminal Code Act 1995* even if it features fictional or cartoon characters. The transmission, storage or downloading of obscene or offensive material may also put staff at risk of breaching discrimination laws.

Inappropriate and prohibited material includes:

- text, graphics, video or other material of a sexual nature (including pornography and other adult material such as swimsuit or lingerie modelling);
- offensive language or offensive material, including jokes or commentary of a sensitive nature (e.g. about race, age, gender, disability, marital status, sexual orientation, religion, political beliefs or appearance);
- racially offensive material which, if communicated, would constitute offensive behaviour within the meaning of section 18C of the Racial Discrimination Act 1975;

- material that is defamatory, abusive or constitutes a form of unlawful discrimination or potential harassment;
- gambling or financial market trading material;
- dating and chat rooms;
- malicious software;
- criminal skills material including instructions on how to obtain drugs or stolen property, or create weapons or explosives; or
- illegal websites blocked by Australian Government.

Filtering and monitoring of prohibited use

Shared Services ICT maintains an Internet content filter to prevent ACT Government staff from accessing inappropriate or prohibited material. This filter intercepts web requests and determines whether the site being accessed is acceptable under the terms of this Policy. If the filter determines that a site falls outside the Policy, the site will either be blocked, or a warning screen will be displayed advising that the site appears to be in breach of the Policy.

If you proceed to view an inappropriate or prohibited web site, your access will be permanently recorded in a security log and investigated.

If you accidentally access prohibited material and were not warned, for example if you were redirected from a legitimate website that has been compromised, immediately close the browser.

Reporting offensive material

Report any message you believe is offensive, humiliating or intimidating that you reasonably believe was deliberately sent to you.

Report these incidents to your supervisor or to Shared Services ICT Security. All complaints will be addressed promptly and treated impartially and confidentially.

Excessive use

Excessive personal use of ICT resources is prohibited, particularly where it impacts on your official duties or on ACT Government operational effectiveness, clients, staff or resources.

Do not use ACT Government ICT resources to:

- access streaming media (e.g. online music and video content) unless it is work-related;
- create or post to personal blogs or personal web pages; or
- conduct a private online business (such as selling on eBay or share trading).

Excessive web browsing unrelated to official business during work hours is improper. Use good judgement and seek advice from your supervisor if you are unsure what constitutes “excessive” personal use.

Spam and suspicious email

Do not forward or reply to any spam message (i.e. unsolicited commercial email).

Do not send unauthorised bulk email or “chain messages”.

Do not send email:

- seeking personal gain;
- promoting an outside business;
- encouraging others to engage in industrial action; or
- supporting a partisan political purpose, such as a political candidate or ballot position.

If you receive email of this nature from other staff, report these incidents to your supervisor.

Information security

Information security is governed by the *Public Sector Management Act 1994*, in Section 9(m):

- Do not disclose, without lawful authority, information acquired by or from any document to which you have access because of your employment.

Further detail is provided by the *Public Sector Management Standards 2006*, in Part 2.4 (18):

- Do not disclose confidential information without approval of the delegate.

The ACT Protective Security Policy Framework (ACT PSPF) provides more detail about the definition of confidential information and how it must be protected by all staff.

Do not disclose official information

Only release official information to organisations and individuals with a demonstrated **need to know**.

Apply the need to know principle when disseminating official information, even if you are communicating with other staff.

Do not disclose official information to unauthorised recipients. Authorisation to disclose official information to recipients, including the public, must first be obtained from delegate who owns the information.

If you receive official information by mistake:

- immediately notify the information owner, and
- delete the information, e.g. the email message and any attachments.

Information Privacy

All staff are bound by the *Information Privacy Act (ACT) 2014* and Territory Privacy Principles (TPPs) when handling the personal information of any individual. You must be particularly careful to:

- use personal information only for the purpose for which it has been provided
- take reasonable steps to protect personal information from loss or disclosure, and
- never disclose personal information to unauthorised recipients.

Always follow the applicable ACT and Commonwealth legislation when using personal information related to health, education, legal matters, child protection, corrections and community services.

Freedom of Information requests

The *Freedom of Information Act 1989* defines the circumstances under which official information may be provided to a member of the public.

Do not release official information that is exempted from FOI requests.

Copyright and intellectual property

Do not use ICT resources for the reproduction of copyright material for the purpose of further distribution, except for what is allowed under relevant Exceptions, Statutory and Voluntary Licences within the *Copyright Act 1968 (Cth)*.

Taking into consideration what is allowed under relevant Exceptions, Statutory and Voluntary Licences within the *Copyright Act,* you must:

- Identify copyrighted material as such
- Respect the intellectual property rights of the owners of copyrighted material, and
- Obtain written permission from the copyright owner to reproduce copyrighted material, including trademarks and logos, text, sound, photographs, illustrations and other graphic images, audio and video files.

A guide to copyright in Education can be found at http://www.smartcopying.edu.au

Information classification

You must apply protective labels to official information that is classified or sensitive in accordance with the ACT PSPF.

You must apply extra protection to classified or sensitive information when it is handled electronically, in accordance with the *ICT Security Policy*.

Sensitive and classified email

Protectively mark each email you send using the approved classification tool built into the email client. Do not remove or change the protective marking unless you are the information owner and are reclassifying the message.

Do not use email to send information that is classified or protected with a DLM (such as **Sensitive** or **For Official Use Only**) to recipients outside the ACT Government network, including your own personal email accounts.

When handling official information, you must protect it with measures that match the information's value, classification and sensitivity.

If you need to send classified or sensitive information to outside recipients, consult with Shared Services ICT Security for advice on the best way to do so. Approved secure communication options exist including file encryption and encrypted media.

Cloud services

ACT Government will from time to time engage external service providers to handle official information. However, the ACT Government is still required to safeguard this information, and Shared Services ICT actively assesses and manages the security posture of these providers before and during their use in accordance with the Whole-of-Government ICT Security Policy.

Do not engage cloud service providers who do not comply with ACT and Commonwealth law.

Do not engage a cloud service provider for official purposes without approval from the Director General or their delegate. Reasonable personal use of cloud services is permitted, provided it is not **prohibited use** as defined by this policy.

Do not transfer official information to a cloud service provider without approval from the Director General or their delegate.

Security practices

You are responsible for security practices to protect ACT Government information and ICT resources.

- Use a complex password or personal identity number (PIN) on all mobile devices (e.g. laptops, tablets and smartphones) that are vulnerable to loss or theft. “Password123” or “123456” are examples of extremely poor and easily-guessed passwords and PINs.
- Do not re-use a password for an ACT Government ICT resource when accessing a website.
- Do not send sensitive or classified information to external parties unless it is appropriately protected.
- Do not send ACT Government information to private email accounts.
- Lock computers when not in use to prevent unauthorised use by others. If the computer is shared, you must log off the computer before it is used by others.
- Do not download, install or run unauthorised security programs or utilities which reveal weaknesses in the security of a system.

Password security

You are responsible for any breach of an ACT Government ICT resource using your password.

You are responsible for setting, changing, and securing your passwords in accordance with this policy and the *Password Standard*.

Do not reveal the passwords you know to **anyone**, including a supervisor or manager, Help Desk, colleagues, family, friends or strangers. Do not:

- discuss a password in front of others,
- send a password in email or other form of electronic communication (e.g. text, chat), or
- type a password in a questionnaire or security form.

Do not use the same password or PIN for more than one user account or device. In particular:

- Do not use personal passwords or PIN numbers for ACT Government accounts or devices, and
- Do not use ACT Government passwords or PIN numbers for personal accounts or devices.

If you must write down a password, ensure that the written password is physically secured using a method endorsed by Shared Services ICT Security.

If you must store a password online, ensure that it is properly encrypted using a system endorsed by Shared Services ICT Security.

Security awareness

All staff engaged by the ACT Government are responsible for security on a day to day basis and must be aware of their responsibilities under this policy.

- Read and abide by this policy for the term of your employment or contract.
- Sign an Acceptable Use Agreement form acknowledging that you have read this policy and submit your form to your ACT Public Service supervisor for recordkeeping.
- Attend security awareness training when instructed to do so by your supervisor.
- Support and foster a positive security culture with your colleagues.

Security leadership

All supervisors must provide leadership to help achieve good security practices and ensure that their staff are aware of their responsibilities under this policy.

- Provide the current version of this policy to your staff,
- Ensure staff have signed their Acceptable Use Agreement form and send completed forms to Shared Services HR for recordkeeping,
- Ensure staff attend security awareness training when directed to do so by a delegate,
- Ensure all staff know how to classify information and apply protective markings,
- Ensure staff have an appropriate level of security clearance to perform their duties, and
- Ensure staff with security specific duties receive additional appropriate training.

Security incident reporting

All staff must report security incidents to the appropriate channels (Table 1) as soon as possible. This applies to incidents that are personally detected by you or are referred to you, for example, by a customer or an external organisation.

Do not discuss security incidents with media, the public or staff outside these reporting channels, unless authorised to do so by a delegate.

Table 1: Security incident reporting channels

Incident type	Reporting channel			
	Supervisor	Service Desk	Agency Security Advisor	IT Security Advisor
Lost, stolen or damaged ICT asset	●	●		
Suspicious email or website behaviour	●	●		
Suspicious text message or phone call	●	●		
Threatening email, message, phone call or parcel	●		●	
Inappropriate or prohibited use of ICT	●			●
Data spill, breach or leak	●			●
Observed ICT system vulnerability	●			●
Major ICT incident including outage or vandalism of a website	●			●

Copying or installing software on ACT Government computers

Follow the appropriate process within your directorate if you need to install software. Your supervisor or your embedded Shared Services ICT Manager can assist.

Do not copy or install software on ACT Government computers unless you have obtained approval to do so. This applies to all software, including software that is privately owned or obtained from the Internet, online services or portable media such as CD/DVD or USB key.

Malicious software and viruses

Content that is intentionally or accidentally downloaded from websites or received by email may contain malicious software ("malware") such as viruses. All ACT Government computers have anti-virus software installed to automatically check downloaded files, but this is not a guaranteed to identify all malware.

Do not to download untrusted content from websites or removable media to an ACT Government computer.

When it is necessary to download files, only do so from known or trusted sources.

Be cautious when opening email attachments, especially you do not know the sender, or if the sender is not an ACT Government staff member.

Avoid visiting compromised websites that harbour malware. They can be hard to tell at a glance, but Internet Explorer is configured to warn ACT Government users before downloading potentially unsafe content. **Pay attention to these warnings.**

If you suspect an ICT resource has been infected with malware (e.g. a warning is displayed, or your computer behaves erratically or runs very slowly), contact the Shared Services ICT Service Desk immediately.

Network and local drives

Network drives, including personal drives (usually the H drive) are part of the publicly funded resources provided for official ACT Government business use.

Staff must not save software and/or large personal files to any network drive. These drives are regularly monitored, particularly when disk space is at a premium. Graphics, music, video files and '.exe' files will be targeted.

Personal use of ACT Government ICT resources is not considered private. Staff do not have the same personal privacy rights when using these devices as they would if they were using private communication devices. This means that employees reasonably suspected of abusing personal use of employer-supplied communication devices may be asked to explain their actions.

Staff should be aware that the same general restrictions apply to personal (C) drives as for H drives. They must not store on their C drive prohibited or inappropriate material, software or material that is subject to copyright.

Note that the directorate may prohibit storing and data – personal or corporate – on the H drive. Staff should be aware of their directorate policy in this regard.

Online transactions

You must ensure that an appropriate level of security exists for any commercial transaction over the Internet that they undertake during their work.

As with telephone orders, proper authorisation for purchases must be first obtained. Online purchases normally involve the use of credit or charge cards, and staff must pay due regard to conditions regulating their use.

Compliance

Logging and monitoring

Logging is the automated collection of transaction records. It is active, ongoing surveillance performed by Shared Services ICT Security. This Policy describes the way in which employees' activities are monitored and how staff are informed that this monitoring is being carried out.

ACT Government monitors staff use of Government computers and ICT systems by:

- maintaining logs, backups and archives of activities on all ICT resources including computers, laptops, smartphones and tablets,
- monitoring email server performance and retention of logs, backups and archives of emails sent and received through ACT Government servers, and
- retaining logs, backups and archives of all Internet access and network usage.

Shared Services ICT will not disclose the contents of monitoring to a person, body or directorate (other than the individual concerned) unless one or more of the following applies:

- the staff member is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or directorate,
- they have consented to the disclosure,
- Shared Services ICT believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person,
- the relevant directorate Executive has requested monitoring or investigation;
- the disclosure is required or authorised by or under law, or
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Shared Services ICT may log computer activity:

- for system management and planning,
- to ensure compliance with ACT Government policies,
- to investigate conduct that may be illegal or adversely affect ACT Government employees, or
- to investigate inappropriate or excessive personal use of ACT Government ICT resources.

Under the provisions of the *Workplace Privacy Act*, employers must – upon being requested by the worker – provide access to the worker's surveillance records. Workplace surveillance records will be kept in accordance with the requirements of the *Territory Records Act*.

Password auditing

Shared Services ICT Security may audit passwords to assess and enforce compliance with this policy and with the Password Standard. Password audit results are reviewed by Directorate Security Officers and the ACT Auditor-General.

Investigations

Shared Services ICT Security can access and investigate the logs of all of staff activity including:

- the URLs or website addresses of sites visited, the date and time they were visited and the duration of site visits and logs, and
- email messages and attachments, including backups and archives of emails, whether they are current or have been deleted by the user.

Shared Services ICT Security in consultation with the directorate Executive may authorise the investigation of user logs if there is a perceived threat to:

- ACT Government ICT system security,
- the privacy of ACT Government staff,
- the privacy of others, or
- the legal liability of the ACT Government.

These records can be called up and cited as a chain of evidence in legal proceedings and actions following virus attacks. Access will be fully logged and documented.

Exemptions

Where research and investigations are proposed or undertaken that would be likely to breach this Policy, the purpose, scope and design of work being undertaken may require prior approval through the *ICT Policy Waiver Process*. Ask your supervisor or an ICT Manager.

Inappropriate use

In the absence of an explicit Waiver or approval from the Supervisor, the use of ICT Resources for activities that might be inappropriate is forbidden and may lead to disciplinary action being taken against the staff member.

Prohibited use

In the absence of a formal Waiver or approval from a supervisor, prohibited use of ICT resources will lead to disciplinary action and legal proceedings being taken against the staff member.

Consequences

ACT Government ICT resources support many crucial activities for the ACT community, including hospitals and emergency services. Shared Services will take all legally allowed steps it deems appropriate to remedy or prevent activities that endanger the safety of those ICT resources.

Breach of this policy may constitute misconduct under the PSM Standards. Disciplinary action can include counselling, formal warning, conditions placed on continuing service, deductions from salary, changes to employment contract or termination of engagement.

Evidence of prohibited activities will be provided to law enforcement as soon as they are detected. Depending on the severity of the offence, suspects can be placed under arrest and prosecuted under ACT and Commonwealth law.

ICT Acceptable Use Agreement

I, ……………………………………………………………………………………….

(FULL NAME in BLOCK LETTERS and INK)

(a) acknowledge that I have read and understood the *Whole-of-Government Acceptable Use of ICT Resources Policy* and the *Workplace Privacy Act 2011*

(b) agree to abide by the requirements for access and use of these resources

(c) acknowledge that the ACT Government may access my user logs if there is a perceived threat to the:

- Security of ICT resources or information assets
- Privacy of staff
- Privacy of others
- Legal liability of the ACT Government.

This signed acceptance is valid for the period of employment with the ACT Government, or until a revised statement is deemed to be necessary as determined by the ACT Government.

Signature: ....

Date: ....

Section/School: ....

Position Held: ....

AGS No: ....

Supervisor Name: ....

Note: Your full name must match personnel records of Shared Services. Do not use abbreviated or nicknames unless it is your formal name.

Scan and email this form when completed to your ACT Public Service Supervisor.

Glossary

Term	Definition
Unofficial information	Information created for personal purposes by staff, which does not represent a view of the ACT Government or relate to its official business.
Official information	Information that relates to official ACT Government business that can only be released with approval from the Director General or their appointed delegate.
Public information	This is official information that has been approved by the Director General or their delegate for release to the public. Examples might include public event information or community health advice.
Unclassified information	This is official information that if compromised would have low impact on the Government, a business entity or an individual. It does not need additional protection.
Dissemination Limiting Markers	Information classified with a Dissemination Limiting Marker (DLM) requires additional protection due to its sensitivity or enactments of secrecy in ACT or Commonwealth law. If compromised, this information could cause limited damage to the ACT Government, a business entity or an individual. The DLMs used by the ACT Government are defined in the ACT PSPF and include: For Official Use Only Sensitive Sensitive: Personal Sensitive: Legal Sensitive: Cabinet Sensitive: Auditor-General New DLMs must not be created without the authority of the ACT Attorney-General.
Sensitive information	The term “sensitive information” is used to denote any information with DLM starting with Sensitive.
Confidential information	“Confidential” or “X-in-Confidence” no longer exist as ACT security classifications. The term “confidential information” can be interpreted as any information with a DLM, particularly For Official Use Only.
Inappropriate (use or material)	Usage or material that is: • offensive • inappropriate for use or access by public sector staff or agencies by reason of its nature or content, or • restricted by a directive to staff.
Prohibited (use or material)	Usage or material that could: • harm the reputation of the ACT Government • be misleading or deceptive • result in victimisation or harassment • lead to criminal penalty or civil liability, or • be reasonably found to be offensive, obscene, threatening, abusive or defamatory.
Malware	An abbreviation for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Metadata

Owner	Senior Manager, ICT Security
Authority	Executive Director, Shared Services ICT - Executive responsible for ICT Security
Location	http://sharedservices/actgovt/ICTdocs/Acceptable Use Policy V2.6.docx
Review cycle	This document should be reviewed annually or when relevant change occurs to technology, business or the threat environment.
Associated documents	ACT Protective Security Policy Framework 2017

Revisions

Version	Published	Details	Author	Approval
1.0	12/2004	Initial release based on ACTIM's Acceptable Use of IT Resources Standard	A Mayberry	Manager, Security
1.1	01/2004	Additional information added about distribution of inappropriate messages	A Mayberry	Manager, Security
1.2	10/2006	Minor revisions to formatting, changed IT to ICT and HR&CS to BSS.	Policy Office	Endorsed by Policy Office
2.0	06/2009	Major re-write to change the focus to Acceptable Use	Policy Office	Shared Services Governing Committee
2.1	08/2011	Changes to reflect new Shared Services ICT structure and Workplace Privacy Act 2011	Policy Office	A/g GM, Shared Services ICT
2.2	08/2012	Changes to reflect titling of ED and review currency of document	P Major	ED SS ICT
2.3	04/2013	Updated to include Instant Messaging. (not published on portal)	P Major	ED SS ICT
2.4	11/2014	Add Bolden James classifier to Header & Footer. 'PSP&G' to 'PSPF'. 'Privacy Act 1988' to 'Information Privacy Act 2014'. Cosmetic changes	P Major G Tankard	ED SS ICT
2.5	01/2017	Consolidated, revised for cloud and retitled	S Callahan	ED SS ICT
2.6	01/2019	Updated Acknowledgement Form for Supervisors	C Callahan	CISO SS ICT

ACT Government

CMTEDD
Chief Ministers, Treasury and Economic Development Directorate

Version 2.6, 08/01/2019