Acceptable Use of ICT Resources Policy

ACT Health

Version 2.0

March 2011

ACT Health Portfolio Executive

Contents

Introduction

Purpose

This document outlines the acceptable use of Information and Communications Technology (ICT) resources for ACT Government employees.

It is issued by the Shared Services Governing Committee with the agreement of all ACT Government Agencies. All ACT Government staff are hereby directed to comply with its requirements.

Background

ACT Government ICT resources and the services accessible on them are provided to you to carry out tasks related to your job.

It is the intent of this document that the acceptable use of ICT in the ACT Government is overseen and managed by local supervisors. These supervisors will take the responsibility of escalation as deemed necessary in the event of any continuing and ongoing policy breaches. Supervisors and managers are also advised to remind staff of the importance of abiding by this Policy and the possible consequences of inappropriate behaviour.

This Policy is based on two basic principles:

- you should behave in a way that accords with the *Public Sector Management Standards* (Part 2.5) and the statement of *Ethics in the ACT Public Service,* and
- you should not waste the ACT Government's money.

This second dot point is the reason for many of the restrictions on Internet use in this Policy: excessive Web browsing is not a productive use of your time. More importantly, because the Government pays for all its Internet traffic, some Web usage (particularly multimedia downloads and video and audio streaming) can become quite costly.

Roles and responsibilities

Role	**Responsibilities**	**Position**
Supervisor	Make staff aware of their responsibilities under this Policy. Initiate action as necessary when they become aware of non-compliance with this Policy. Approving in writing requests for use normally prohibited by Whole-of-Government and Agency policies	ACT Government employees supervising other staff.
User	Use ACT Government ICT resources, in accordance with the policy requirements set out above.	Permanent and temporary ACT Government employees Non-government staff including contractors and consultants.

Scope

This Policy applies to:

- permanent and temporary ACT Government employees
- non-government staff including contractors and consultants using ACT Government resources.

The Policy applies to the use of desktop devices and portable devices such as laptops and mobiles / PDAs.

Glossary

Term	Definition
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 • that staff have been warned not to carry out or access and Without limiting the above inappropriate online resources include: • dating sites • chatrooms (except those that are work-related) • gambling sites • sites that feature adult content or • sites promoting crime or terrorism.
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.
Prohibited (use or material)	Usage or material 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.

Note: other terms may be found in the InTACT Glossary of Terms.

Policy

1. Awareness

It is the duty of every Supervisor to ensure that their staff are aware of their responsibilities under this Policy. Staff members joining the ACT Government will be required to sign a document (refer to Attachment A for a template that can be used) stating that they have seen a copy of the Policy and are aware of their responsibilities.

2. Legal and regulatory requirements

You must ensure that Confidentiality, Privacy and Commercial-in-Confidence Standards, Practices and Requirements are applied to the use of ICT equipment and the storage, retrieval, access and dissemination of information.

You should be aware of the requirements of section 9 of the *Public Sector Management Act 1994* (the Act)and the *Public Sector Management Standards* (Part 2.5), which binds ACT Public Servants and *Ethics in the ACT Public Service,* which provides official guidance on ethical requirements. In summary, these stipulate that you must:

- ensure that you do not access, download or store inappropriate or prohibited material (see definitions of "inappropriate" and "prohibited" in the Glossary)

- not save any software or large personal files to any network or personal disk drive
- ensure that personal correspondence and activities do not interfere with your duties.

There will be occasions when staff of some agencies will have a business need to access resources that would normally be prohibited under this policy. In such cases, they should ensure that they have prior approval from their Supervisor for such access.

3. Appropriate use

Reasonable private use of ACT Government ICT resources is a privilege.

If you use ACT Government ICT resources for personal reasons, you should ensure that such use is kept to a minimum. As a guideline, resources should only be used for personal reasons outside working hours, and then for a maximum of 45 minutes per day.

In accordance with the requirements of the Act you must avoid improper use and waste and extravagance in managing the property of the Territory. You must be scrupulous in the way in which you use Territory resources, including office equipment, telecommunications and information technology. The *Public Sector Management Standards* cover the proper and effective use of resources and you should familiarise yourself with these.

Using ACT Government ICT Resources for activities that might be inappropriate is forbidden and may lead to disciplinary action being taken.

4. E-mail

You must:

- ensure that personal correspondence does not interfere with your duties and wherever possible deal with this correspondence outside working hours
- not interfere with the work of other employees or tie up facilities required for legitimate purposes
- ensure that you regularly clear your Inbox of all personal messages
- consider whether any personal communication should include a disclaimer making it clear the opinions expressed are your own and do not represent the ACT Government.

If you receive an e-mail message in error, please:

- immediately notify the sender by return e-mail
- delete the message and any attachments.

If you receive any spam message (ie unsolicited commercial e-mail) you should under no circumstances reply to it.

Unauthorised widespread mail-outs or chain letters are not permitted.

You should be wary of using e-mail to send confidential information to other persons, either inside or outside the ACT Government network. If there is a need to transmit confidential information such as patient information by e-mail, outside ACT Government you should encrypt the message and any confidential attachments using an approved email encryption product. InTACT ICT Security and ICT Health Client Services can advise you on what products are available.

You have a right and obligation to report a message that you believe is offensive, humiliating or intimidating that you reasonably believe was deliberately sent to you, other than spam. All complaints will be treated impartially and confidentially, and will be addressed promptly. You can make your complaints to your supervisor or the Manager, InTACT ICT Security.

Any type of unethical or unlawful use of ACT Government ICT resources may result in immediate suspension of your access to the service and you may be subject to disciplinary actions or legal proceedings.

5. Malicious software and viruses

Material downloaded or received over public networks may contain viruses or other malware. When it is necessary to download files, only do so from known or trusted sources. All ACT Government computers have anti-virus software installed and this automatically checks all downloaded files.

You should show extreme caution when opening email attachments, particularly if they have been sent to you by someone you do not know, or if the sender is not an ACT Government staff member.

Your computer may also be infected by software loaded from websites, either intentionally or accidentally. Be careful not to download any software from such sites.

If you suspect that your computer has been infected with a virus (for instance if it runs very slowly or starts to behave erratically) you should contact the InTACT Service Desk on x75555 immediately.

6. World Wide Web usage

Excessive Web browsing unrelated to official business during work hours is prohibited. The term "excessive" is to be negotiated at the local area between supervisors and staff.

You must not, during working hours:

- access online media streaming sites (eg radio, music and video broadcasts) unless they are work-related
- create and post to personal blogs
- creating personal web pages
- conduct a private online business (including dealing on eBay or similar sites, or share trading).

You may, as long as it does not impact your work:

- perform personal online banking
- contribute to work-related online discussion groups.

7. Prohibited use

You must not create, send or access 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.

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

In addition to prohibited material, there is a category that is considered inappropriate for access through ACT Government ICT resources. To address this, InTACT has deployed a content filter to monitor Internet access by ACT Government staff. 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. Depending on the Agency of the user, the content filter will warn or block access to categories of websites including:

- adult content
- gambling
- chat rooms
- dating
- crime/terrorism
- violence/undesirable activities
- malicious
- government blocking list (illegal websites)
- swimsuit/lingerie models.

Should you need to access legitimate sites for your work but you find them filtered, you will need to seek permission through the Director of Operations, Human Resource Management Branch, to access the sites.

You must not create, send, access, download or store inappropriate or prohibited material unless it is part of your official duty to do so.

8. Copying or installing software on ACT Government computers

Software of any description may not be copied or installed on ACT Government computers unless you have specific approval to do so. This applies to all software, including software that is privately owned or obtained from the Internet, on-line services or portable media such as CDs/DVDs and USB keys.

If you have a need to install any software, you should follow the appropriate process within your agency. For information on this, contact your Supervisor in the first instance and then the Agency ICT Manager.

9. Communications

Any staff member who initiates fraudulent, unlawful or abusive communication may be subject to disciplinary action and possible criminal prosecution.

While it may be unavoidable to open inappropriate messages, further internal or external distribution of such messages must not occur, other than to an appropriate investigating authority such as InTACT ICT Security.

You may be individually liable if you aid and abet others who discriminate against, harass or vilify colleagues or any member of the public.

10. Confidentiality

You should:

- be aware that unauthorised disclosure of confidential information is a breach of the Code of Ethics and may be a breach of the Privacy Act and the ACT Health Records (Privacy and Access) Act 1997.

- apply confidentiality, privacy and commercial-in-confidence standards, practices and requirements to the storage, retrieval, access and dissemination of information.
- apply confidentiality, privacy and classification standards (*ACT Govt Protective Security Policy and Guidelines*), practices and requirements to the storage, retrieval, access and dissemination of information.

Storage of classified or sensitive information electronically requires care. For example, carrying information on a disk or other removable storage device means that you must treat that device with the same care as a classified file. Extreme care must be taken with the use of e-mail in these circumstances to avoid unauthorised publication of classified and sensitive official information. For more information on this, see the *Encryption Policy*.

11. Passwords

Your use and management of passwords must be in accordance with the *Password Policy*.

12. Logging and monitoring

Logging refers to the automated collection of transaction records. Monitoring includes active, ongoing surveillance by InTACT Security under the ACT Government IT Security Adviser.

InTACT Security have access rights to logs of all of your activity including:

- backups and archives of all files, including e-mails, which are current and those that have been deleted by the user
- e-mail messages and attachments
- the URLs or website addresses of sites visited, the date and time they were visited and the duration of site visits and logs.

InTACT Security in consultation with the Agency Executive may authorise access to user logs in the event that there is a perceived threat to:

- ACT Government ICT system security
- the privacy of ACT Government staff
- the privacy of others
- 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.

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

- you are reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or agency
- you have consented to the disclosure
- InTACT 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 Agency Executive has requested monitoring or investigation
- the disclosure is required or authorised by or under law
- 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.

InTACT may log on a random or continuous basis:

- 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
- to investigate inappropriate or excessive personal use of ACT Government ICT resources.

13. Security

Some simple steps you can take to protect your communication and ACT Government ICT resources include:

- using password or personal identity number protection on all mobile devices (eg laptop computers, phones and PDAs) that are vulnerable to theft
- not sending classified information eg Cabinet-in-Confidence documents, Tax File Numbers (TFN), passwords, PINs and other sensitive information to external parties via e-mail unless appropriately encrypted
- not sending ACT Government information on private e-mail systems
- not downloading, installing or running security programs or utilities which reveal weaknesses in the security of a system. For example, you must not run password cracking programs on ACT Government ICT resources
- locking computers when not in use to avoid use by others. If the computer is shared, log off the computer to facilitate use by others
- not using a password that you use on any ACT Government ICT resources to access any Internet sites.

14. Online transactions

You must ensure that an appropriate level of security exists for any commercial transaction over the Internet that you undertake in the course of your 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 you must pay due regard to conditions regulating their use.

15. Intellectual property rights - including copyright

Taking into consideration what is allowed under relevant Exceptions, Statutory and Voluntary Licences within the *Copyright Act 1968 (Commonwealth)* you must:

- ensure that the intellectual property rights of the providers of material are respected
- 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. Copyrighted material should be identified as such.

Reproduction of copyright material for the purpose of further distribution outside of what is allowed under relevant Exceptions, Statutory and Voluntary Licences within the *Copyright Act 1968 (Commonwealth)* is illegal and the use of ACT Government resources for this crime may render the Government liable to prosecution.

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

16. Network and local drives

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

You 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. In particular, graphics, music and video files, and '.exe' files will be targeted.

Reasonable personal data, such as CVs or job applications, may be temporarily stored on your computer's local C: drive, noting that C: drive is neither secure nor backed up. Such personal files should be stored on personal storage such as a USB thumb drive or a CD removed from C: drive as soon as practicable. Corporate (i.e. business-related) files must not be stored on C: drive.

H: drive should not be used for the storage of personal or corporate files other than e-mail PST files.

Corporate information should be stored on Q: drive in an appropriate place with appropriate access control. Folders with access restrictions can be requested through the IT Portal.

Personal use of ACT Government ICT resources is not considered private. You do not have the same personal privacy rights when using these devices as you would if you 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.

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

Note that your Agency may prohibit storing and data – personal or corporate – on your H drive. You should be aware of your Agency policy in this regard.

17. Record keeping

Business communications that are sent electronically (eg e-mail messages) become official records, and are therefore subject to statutory record keeping requirements. Advice on the retention and storage of electronic records can be found in Records Advice 3 and 5 at http://www.territoryrecords.act.gov.au/recordsadvice

18. Access

Access to ACT Government ICT resources is to be used only for the purpose for which you are authorised. This means that you must not attempt to access any data or programs that you do not have authorisation or explicit consent to access.

Any type of unethical or unlawful access may result in immediate suspension of your access to these services and you may be subject to disciplinary actions and legal proceedings.

In particular, access to pornography, hate sites and gambling sites is prohibited. Staff are reminded that by accessing some Internet sites, you may inadvertently be re-directed to an inappropriate site. If this occurs, you should immediately exit the site.

If you have any queries regarding access to ICT resources, contact the Agency ICT Manager or discuss the issue with your supervisor.

Compliance

1. Exemptions

Where research and investigations are proposed or undertaken which would be likely to breach these guidelines, the purpose, scope and design of work being undertaken requires prior approval of the ACT Health Human Research Ethics Committee (ACTHREC) before proceeding. Initial enquiries should be made through the ACTHREC secretariat (Joan Jensen).

If you are planning to access electronic health records for research purposes Ethics approval will be required. For more information, please see the ACT Health Human Research Ethics Committee Guidelines.

2. Inappropriate use

In the absence of an explicit Waiver or approval from your Supervisor, the use of ACT Government ICT Resources for activities that might be inappropriate is forbidden and may lead to disciplinary action being taken against you. See the Glossary for a list of inappropriate uses of ICT resources.

3. Prohibited use

In the absence of an explicit Waiver or approval from your Supervisor, prohibited use of ACT Government ICT resources will lead to disciplinary action and legal proceedings being taken against you. See the Glossary for a list of prohibited uses of ICT resources.

Associated documents

- Public Sector Management Standards (Part 2.5)
- Ethics in the ACT Public Service
- ICT Policy Waiver Process
- Password Policy
- Encryption Policy
- Remote Access to the ACT Government ICT Environment Policy
- Privacy Act 1988 (Commonwealth)
- Health Records (Privacy and Access) Act 1997;
- Copyright Act 1968 (Commonwealth)
- ACT Govt Protective Security Policy and Guidelines
- Territory Records Office Records Advice 3
- Territory Records Office Records Advice 5

ACT Health Policies:

- ICT Security Policy
- ACRS Network and Information Systems
- Public Health Records and Information Policy and Disposal Authority
- Release of Client Information to Clinicians
- Data Quality Policy
- Data Release Policy

- Data Repository Policy (Draft)

Contact officer

For all queries about this policy, contact ICT Health Client Services on 6205 3999.

Attachment A – Template

Acceptable Use of IT Resources

I, …………………………………………………………………..………………….

(PRINT FULL FIRST, MIDDLE & SURNAME – BLOCK LETTERS and in INK)

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

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

(c) acknowledge that the ACT Health may authorise access to user logs in the event that there is a perceived threat to the:

- System security
- Privacy of staff
- Privacy of others
- Legal liability of the ACT Government.

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

Signature: …………………………………………………………………………..

Date: ………………………………….

Business Unit: ……………………………………………………………….

Position Held: ………………………………………………………………

AGS No: ……………………………………………………………………….

Note: Use of the full name is important. It must match personnel records of Shared Services. Do not use abbreviated or nicknames (eg Shelley for Michelle, Meg for Margaret, etc.) unless it is your formal name.

Please lodge this form with your Business Unit Manager

Appendix A

Metadata

Owner:	Chief Information Officer
Document location:	ACT Health Policy Register
Review cycle:	This policy should be reviewed every 12 months or when associated ACT Government policies or standards are amended.

Note: This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the intranet version prior to use.

Amendment history (Whole-of-Government Policy)

Ver no.	Issue date	Amendment details	Author	Approval
1.0	22 Dec 2004	Initial release, based on ACTIM's *Acceptable Use of IT Resources Standard*	Anne Mayberry	Manager, Security
1.1	18 Jan 2004	Additional information added about distribution of inappropriate messages (Communications paragraph)	Anne Mayberry	Manager, Security
1.2	27 Oct 2006	Minor revisions to formatting, changed IT to ICT and HR&CS to BSS.	Policy Office	Endorsed by Policy Office
2.0	June 2009	Major re-write to change the focus to Acceptable Use	Policy Office	Approved by Shared Services Governing Committee