**Canberra Health Services**

**Procedure**

**Information and Communication Technology Resources: Acceptable Use**

|  |
| --- |
| Contents |

[Contents 1](#_Toc74208111)

[Purpose 2](#_Toc74208112)

[Alerts 2](#_Toc74208113)

[Scope 2](#_Toc74208114)

[Section 1 – Roles and responsibilities 3](#_Toc74208115)

[Section 2 – Use Local Drives and Network Access Storage 5](#_Toc74208116)

[Evaluation 6](#_Toc74208117)

[Related Policies, Procedures, Guidelines and Legislation 6](#_Toc74208118)

[References 7](#_Toc74208119)

[Definition of Terms 7](#_Toc74208120)

[Search Terms 7](#_Toc74208121)

|  |
| --- |
| Purpose |

The purpose of this procedure is to provide guidance on the access to and use of Information and Communication Technology (ICT) resources across CHS to support clinical and administrative functions.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Alerts |

This document should be read in conjunction with the Whole of Government (WhoG) Acceptable Use of Information and Communications Technology (ICT) Resources Policy (Acceptable Use Policy), which is managed by Shared Services ICT.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Scope |

This procedure applies to all Canberra Health Services (CHS) employees, visiting health professionals, contractors, students, volunteers and others who use and access CHS ICT resources. In this document, ’ICT resources‘ refers to the resources utilised throughout CHS to communicate, create, distribute, store, and manage information. Examples of ICT resources include:

* CHS-owned devices e.g. computers, laptops, iPads, Toughbooks and mobile devices.
* Electronic files, folders, software and applications
* ACT Government local storage drives (C: drive) and network access storage (Q: drive)
* Including all electronic folders and files contained therein
* Software and applications
* ACT Government email and internet usage
* ACT Government Wi-Fi
* CHS/ACT Government specific applications such as ACTPAS, Clinical Portal
* Removable storage devices e.g. USB sticks, hard disk drives, portable devices and memory cards.

For clarity, this procedure does not apply to users who are using non-ACT Government equipment on the Health free Wi-Fi network.

While mobile communication devices are considered an ICT resource, and as such are covered broadly in this document, specific information for mobile device utilisation within CHS is not in scope for this procedure and can be found in the CHS Mobile Communication Devices Management and Use procedure.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Section 1 – Roles and responsibilities |

**Managers will:**

Inform staff and users:

1. of their responsibilities under the Acceptable Use Policy.
2. of the existence of this procedure.
3. of where to go for information and assistance in locating ICT Services; such as obtaining a user account, resetting passwords, accessing mailboxes.
4. of where information and online forms can be accessed on the CHS Intranet;
*HealthHUB* IT and Data page > IT Portal. Staff and users will be requested to contact their manager or the Shared Services ICT Service Desk if they require further information.
5. for standard requests for access to ICT resources ( for example obtaining access to shared network drives and folders such as the G: and Q: drives), that they should access the Identity and Access Management (IAM) portal from the IAM Service link on the main page of the CHS Intranet. (For details on what staff and users can request and how to request access in IAM, refer to IAM Responsibilities for CHS IT Processes below.)
6. that they should notify the appropriate Executive Director/Executive Group Manager of any suspected or alleged breaches involving non-compliance with the Acceptable Use Policyand/or this procedure. Staff responsible for such incidents should be managed in accordance with CHS Workplace Values and Behaviours outlined in the relevant Enterprise Agreement.
7. of their responsibilities concerning the appropriate behaviour of staff under section 9 of the *Public Sector Management Act* 1994 and the ACT Government/CHS Code of Conduct.

Additionally, managers will:

1. escalate significant incidents, inappropriate access of confidential patient information and serious breaches relating to this procedure to the Senior Executive Responsible for Business Integrity Risk (SERBIR), the Deputy Chief Executive, Strategy, Policy and Planning, People and Culture and relevant HR Business Partners (where there is a potential misconduct-related incident/action).
2. advise staff that possible outcomes for the staff member/user may include:
* Risk Incident Investigation
* Interview and / or counselling
* Formal disciplinary action (Termination of employment/contract or cancellation of service provider arrangements)
* Internal Audit Review.

**Staff and users will:**

1. be aware that at any time CHS or Shared Services ICT can confiscate and retain devices, regardless of ownership, which have been connected to the ACT Government Network or used in the workplace, including but not limited to USB sticks, hard disc drives, portable devices and memory cards. For further information please visit <https://www.territoryrecords.act.gov.au/recordsadvice>
2. not create, send or access information that could damage the ACT Government’s or CHS’ 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.
3. not save software 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 for review.
4. be aware that the same general restrictions apply to personal C: drives as for H: drives. In particular, staff and users must not store on their C: drive prohibited or inappropriate material, software or material that is subject to copyright where CHS or the staff member is not authorised to store such material. Note that CHS may prohibit storage of any data – personal or corporate – on the H: drive.
5. be accountable for their responsibilities in regard to inappropriate access or use of prohibited material which is further detailed in Acceptable Use Policy.
6. seek permission through their manager if they need to access legitimate sites for their work that are filtered, for example research that is associated with breast cancer.
7. where installation of any application, software or ICT hardware is required, contact their manager in the first instance and if approved then lodge a request with the Shared Services ICT Helpdesk.
8. refrain from connecting an ACT Government computer or device to an insecure free/public Wi-Fi network, as this could introduce additional security concerns when dealing with sensitive patient data.
9. be wary of using email to send confidential or sensitive information to other persons, either inside or outside the ACT Government network (for example, information that includes patient details).

**Note**:

Emails within the ACT Government and to any email addresses ending in “.gov.au” or “calvary-act.com.au” are securely encrypted.

All email exchange servers apply some level of encryption to the email during transport between services, however extreme caution should be used when selecting email recipients or entering/typing private email addresses. Security and privacy is hard to ensure if correspondence is sent to an email address that does not end in “.gov.au” or “calvary-act.com.au”. Staff should be careful about sending private and sensitive information to email addresses that do not end in “.gov.au” or “calvary-act.com.au” and should consider alternative communication methods, for example facsimile.

It is permissible for staff to send sensitive medical information relating to patients, to the patient in question, provided the patient has first emailed their permission to receive this information via email. This will not only confirm the patient’s permission has been given but will ensure that the correct email address is being used.

1. be aware that all electronic documents containing Government information are subject to the *Freedom of Information Act* 2016*.*
2. report to a manager any incidents, inappropriate access of confidential patient information or any breaches relating to this procedure. The manager will advise the SERBIR, as appropriate, and notify People & Culture (including relevant HR Business Partner) in relation to the potential misconduct.

**Note**:

Possible outcomes for the staff member/user may include:

* Risk Incident Investigation
* Interview and /or counselling
* Formal disciplinary action
* Internal Audit Review
* Termination of employment/contract or cancellation of service provider arrangements.

Any staff queries regarding access to ICT resources within the CHS should be discussed with their manager in the first instance.

1. Ensure that personal use of technology does not interfere with CHS business requirements.

**Information and Access Management’s Responsibilities for CHS IT Processes include:**

* + - 1. Requesting access to:
* a computer/local area network
* folders on the Q: Drive
* Citrix
* Outlook.
	+ - 1. Removing computer access from an employee or user, at the request of an authorised manager.
			2. Creating a new generic mailbox at the request of an authorised manager.

Requests can be made directly with IAM located at Canberra Hospital or via the Intranet homepage *health*HUB/IT Portal/IAM (Contact details - Ph: 5124 5000; Email: Digital.Support@act.gov.au

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Section 2 – Use Local Drives and Network Access Storage |

1. Corporate information should be stored on the Network Access Storage (Q: drive) in an appropriate place with appropriate access control. Folders with access restrictions can be requested through IAM.
2. Clinical information should not be stored on the Network Access Storage or local drives but should be stored within the appropriate approved clinical information system or the scanned record solution, for example the Clinical Patient Folder.
3. Corporate information stored on removable devices (such as USB sticks, hard disk drives, portable devices and memory cards etc.) must be secured by passwords and encryption.
4. All Network Access Storage, including personal drives such as H: drive, are ACT Government resources provided for official ACT Government business use and are subject to Freedom of Information (FOI) legislation.
5. Reasonable personal data, such as curriculum vitae or job applications, may be temporarily stored on a computer’s local C: drive, noting that the 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 Computer Disk removed from the C: drive as soon as practicable. Corporate, business-related files must not be stored on the C: drive.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Evaluation |

**Outcome Measures**

* significant incidents related to inappropriate access/use of ICT will be escalated
* inappropriate access of confidential patient information and serious breaches relating to this procedure will be escalated.

**Method**

* Yearly review of SERBIR notifications related to inappropriate access to ICT resources
* Regular review of Shared Services ICT reporting to People and Culture.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Related Policies, Procedures, Guidelines and Legislation |

**Policies**

* Protective Security
* Whole of Government Acceptable use of Information and Communications Technology (ICT) Resources
* Whole of Government Mobile Devices
* ACT Government Encryption
* ACT Government ICT Security

**Procedures**

* Mobile Communication Devices Management and Use
* Protective Security (Official Visits by Foreign Delegations)
* ACT Government CHS Code of Conduct

**Legislation**

* *Freedom of Information Act* 2016
* *Health Records (Privacy and Access) Act* 1997
* *Human Rights Act* 2004
* *Work Health and Safety Act* 2011
* *Territory Records Act* 2002
* *Privacy Act* 1988
* *Workplace Privacy Act* 2011
* [*Spam Act* 2003](http://www.acma.gov.au/WEB/STANDARD/pc%3DPC_310296)
* *Public Sector Management Act* 1994

**Whole of Government documents**

* ACT Government Code of Conduct

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| References |

1. ACT Government Acceptable Use of ICT Resources Policy, Version 2.6, 8 January 2019

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Definition of Terms  |

**SERBIR**

Senior Executive Responsible for Business Integrity Risk. The SERBIR in CHS is the Deputy Chief Executive, Strategy, Policy and Planning.

**Users**

Any authorised individual who accesses or uses ACT Government ICT equipment, information systems or applications. This does not include users who access the Health free Wi-Fi network on non-ACT Government equipment.

[*Back to Table of Contents*](#Contents)

|  |
| --- |
| Search Terms  |

ICT, Technology, Acceptable Use, IT, Resources, Computer

[*Back to Table of Contents*](#Contents)

**Disclaimer**: *This document has been developed by Canberra Health Services specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and Canberra Health Services assumes no responsibility whatsoever.*

*Policy Team ONLY to complete the following:*

|  |  |  |  |
| --- | --- | --- | --- |
| *Date Amended* | *Section Amended* | *Divisional Approval* | *Final Approval*  |
| *09 June 2021*  | *Complete Review*  | *Raelene Burke, EGM, People and Culture*  | *CHS Policy Committee* |
|  |  |  |  |

*This document supersedes the following:*

|  |  |
| --- | --- |
| *Document Number* | *Document Name* |
| *DGD-18/019* | *Information and Communication Technology Resources: Acceptable Use Procedure* |
|  |  |