Australian Capital Territory

Corrections Management (Information and Communications Technology) Operating Procedure 2025

Notifiable instrument NI2025–397

made under the

Corrections Management Act 2007, s14 (Corrections policies and operating procedures)

---

1 Name of instrument

This instrument is the *Corrections Management (Information and Communications Technology) Operating Procedure 2025*.

2 Commencement

This instrument commences on the day after notification.

3 Operating Procedure

I make this operating procedure to facilitate the effective and efficient management of correctional services.

Leanne Close APM
Commissioner
ACT Corrective Services

26 June 2025

OPERATING PROCEDURE	Information and Communications Technology
OPERATING PROCEDURE NO.	25.3
SCOPE	Alexander Maconochie Centre

PURPOSE

To provide instructions for ACT Corrective Services (ACTCS) staff to enable detainees to have access to Information and Communications Technology (ICT) in the Alexander Maconochie Centre (AMC).

PROCEDURES

1. Access and conditions of use

1.1. During the induction process, each detainee will be issued with a personalised username and password to access ICT.

1.2. Detainees may gain possession of a games console in accordance with the *Incentives and Earned Privileges Policy*. A games console is considered an ICT device for the purpose of this policy.

1.3. Detainees must not share their username and/or password with anyone else. Detainees can request a password reset if they forget their password, or where they are concerned about the security of their password.

1.4. Detainees are not permitted to encrypt or password-protect any data on any device. They must not use ICT for the following, and may be managed under the *Discipline Policy* for activities including, but not limited to:

a. activity constituting a risk to the safety of any person, or to the security or good order of the AMC
b. revictimising a victim
c. causing distress to the community
d. misuse or corruption of a device/s or operating system
e. use of another detainee's account, or the name and password of another detainee
f. communicating with another detainee, either directly or through a third party
g. installing or modifying any software
h. modifying system settings
i. fraudulent purposes
j. use or circulation of illegal, prohibited or other inappropriate material, including material designed to cause unrest within the AMC, or pornographic material
k. encrypting or password-protecting any data
l. passing information to a third party on behalf of another detainee to circumvent the safety, security, and good order of the AMC

m. attempts to bypass, circumvent security, or access websites not approved for detainees

n. criminal behaviour and/or

o. conducting business.

1.5. Where a detainee has used ICT inappropriately their computer account may be restricted by the Assistant Commissioner, Custodial Operations.

1.6. Detainees can request a review of decisions relating to the restriction of access to ICT systems under the *Detainee Requests and Complaints Policy*.

1.7. Educational providers can arrange for new material to be added or outdated material to be removed from detainee computers by making a request to the Senior Director Detainee Services

a. materials being added or removed must go through the Security Systems team

b. before new material is uploaded to a detainee's profile, the Security Systems team will review the material for relevance to the detainee's education (in consultation with the Senior Director Detainee Services), how the material is to be introduced and that it meets security and cyber safety requirements.

c. the Security Systems team will remove material from a detainee's profile on request.

2. Internet access

2.1. Detainees may access whitelisted internet sites on devices provided at the library.

2.2. Detainees may access to approved websites to:

a. meet their education, vocation or training program requirements

b. access news and information in accordance with section 52 of the *Corrections Management Act 2007*

c. access notified ACTCS policy and procedure documents, legislation and legal resources and

d. access recourses that support rehabilitation and reintegration.

2.3. The list of approved websites will be available on all ICT used by detainees.

2.4. Detainees who require access to a website not already whitelisted, to be able to meet their legal needs, must submit a *Detainee Request Form* to the Director Security Systems and must include the reasons for the requirement.

2.5. In deciding whether to grant or deny a website access request, the Senior Director Detainee Services, in consultation with the Director Security Systems, will consider:

a. whether access is for study purposes and whether the detainee is a current student at the associated educational institution

b. if there are reasonable grounds to suggest that the website is relevant to the detainee's legal needs, including if the detainee is self-representing

c. if alternatives to meeting the detainee's needs are available without approving access to the website for all detainees

d. feedback from the Intelligence Unit to provide details on any relevant factors such as victims, AFP concerns, cyber risks etc

e. feedback from the Security Systems Unit

f. anything else the Senior Director, Detainee Services considers appropriate.

2.6. The detainee will be informed of the final decision and a case note recorded on the detainee's electronic record system.

3. Technical support

3.1. Where a detainee requires ICT technical support, they must submit a *Detainee Request Form* to Executive Support to request assistance. This includes, but is not limited to:

a. requests to repair non-operating or damaged equipment

b. network or connection issues, and/or

c. email or internet access issues.

3.2. There is no provision for ICT technical support if the device is a games console, ICT product, including peripherals, obtained as an incentive under the *Incentives and Earned Privileges Policy*.

3.3. Requests under section 3.1 are to be sent on behalf of the detainee to actcssecuritysystems@act.gov.au for investigation and a response.

4. Monitoring

4.1. All logs, records and archives of ICT system use by detainees may be used as evidence.

4.2. All detainee use of ICT systems and electronic devices may be:

a. archived indefinitely

b. reviewed by automated systems

c. reviewed and audited by authorised ACTCS staff and/or

d. reviewed by authorised external agencies for the purposes of investigating suspected criminal or unlawful activity.

RELATED DOCUMENTS

- Corrections Management Act 2007
- Detainee Requests and Complaints Policy
- Detainee Request Form
- Discipline Policy
- Incentives and Earned Privileges Policy

James Taylor-Dayus
A/g Assistant Commissioner, Custodial Operations
ACT Corrective Services
17 June 2025

Document details

Criteria	Details
Document title:	*Corrections Management (Information and Communications Technology) Operating Procedure 2025*
Document owner/approver:	Assistant Commissioner Custodial Operations, ACT Corrective Services
Date effective:	The day after the notification date
Review date:	Five (5) years after the notification date
Responsible Officer:	Senior Director, Detainee Services
Compliance:	This operating procedure reflects the requirements of the *Corrections Management (Policy Framework) Policy 2024*

Version Control			
Version no.	**Date**	**Description**	**Author**
V1	June-25	First Issued	Y Jansen