8.3 Inmate computers

Policy summary

Access to computers allows an inmate to participate in rehabilitation & educational programs and employment. It also allows them to view legal materials that have been provided on an external storage device.
Inmates must be approved to access computers and be regularly supervised while they are using them.

This policy outlines the circumstances under which an inmate may access a computer:

- as part of their employment in a correctional centre
- to participate in education (internal or external courses) or programs
- to view and/or prepare legal material.

Management of Public Correctional Centres Service Specifications

Service specification	Rehabilitation and Reintegration Safety and Security

Scope

This policy applies to all staff and inmates in NSW correctional centres and those facilities operated by CSNSW.

Table of contents

1 Inmate computers

1.1 Policy

An inmate may be provided access to computers to participate in education and employment programs and to view or prepare legal materials. Access or use for private purposes should not be permitted under any circumstances. Inmate access to computers must be regularly supervised and in accordance with the CSI *Guidelines for Inmate Access to Computers*. Access to computers is withdrawn if an inmate breaches the guidelines.

Computers available for use by inmates are identified by colour:

- Green computers are connected to the Offender Access to Computer (OAC) network and are for education, programs and employment purposes
- Blue computers are non-networked and are for the purpose of viewing and preparing legal documents
- Red computers are non-networked and are for CSI employment purposes, to be issued only under approved circumstances (see part 2.3 below).

An inmate is not permitted to have access to corporate systems or staff computers and must not be permitted to view information on a corporate computer.

1.2 Exclusions

Only the Governor and/or Corrections Intelligence Group (CIG) may decide whether to approve computer access for inmates if they are:

- designated Extreme High Risk Restricted or National Security Interest
- designated Extreme Threat Inmates
- on a restricted management regime such as being managed by the High Risk Inmate Management Committee or
- a high profile or public interest inmate.

2 Approval for access to computers

2.1 Inmate access to green computers (education, programs and employment)

An inmate must be issued a password by the Education Services Coordinator (ESC) or authorised officer via the eForms process. See *CSI Officer Access Network Computers eForm*.

Refer to the *CSI Policy Manual* - section *8.8 Inmate involvement in clerical work* for procedures on how to grant approval for inmates to access green computers for the purpose of employment with CSI.

2.2 Inmate access to blue computers (legal)

This section must be read in conjunction with **COPP section 20.8 *Access to legal resources and documents.***

Blue computers allow inmates to access their legal material that is supplied on an external storage device provided by the inmate's legal representative, an exempt body or a prosecutorial body. The external storage device must be accompanied by a letter which states that the material on the device is relevant to the inmate's current legal matters. The external storage device must be registered on the OIMS Inmate property module as per ***COPP Section 4 Inmate property***.

An inmate is only permitted access to a blue non-networked computer using the generic inmate log-in and password.

2.3 Inmate access to red computers (CSI employment)

This section must be read in conjunction with *CSI Policy Manual Section 8.8 Inmate Involvement in Clerical Work.*

In some circumstances, an inmate may be approved to access a red non-networked computer for participation in CSI employment programs. Approval for use of a red computer must be sought from the CSI Director, Operations Development. Red computers must undergo a monthly security review using the *Inmate Computer Security Check*.

An inmate is only permitted to operate a red non-networked computer using a Student log in and password.

2.4 Inmate access to approved laptops or tablets (legal brief)

Inmates may be approved to access an approved tablet or laptop that will include their pre-loaded legal materials. If an inmate is self-represented they may apply to have access to an approved tablet or laptop by completing an *Inmate access to tablet/laptop* and submitting it to the Functional Manager (FM) accommodation. The FM accommodation must forward the application to accesstojustice@dcj.nsw.gov.au.

If an inmate is not self-represented, their legal practitioner is required to submit the application on their behalf by completing the Inmate Device eBrief scheme application.

All applications will be reviewed by the e-Brief Committee who will assess the inmate's suitability to have access to an approved tablet or laptop. An inmate's suitability for access to an approved laptop or tablet includes (but is not limited to):

- the type of matter (criminal/civil)
- the inmate's classification
- the jurisdiction that the case is currently in (e.g. Local, District, Supreme)
- the inmate's charges
- size of the brief
- if they have access to a blue computer
- the next hearing date
- the anticipated length of the legal proceedings
- any recommendations made by the presiding judge.

If an inmate's application is approved, they must:

- read and sign the *Waiver and release from liability* form and comply with all conditions
- only use the device while in their cell
- ensure that no other inmate has possession or uses the device.

CSNSW retains the right to remove an approved tablet or laptop from an inmate's possession at any time for reasons such as suspected breach of the *Guidelines for inmate access to computer*, breach of security or misuse.

Content on an approved tablet or laptop is restricted to the inmate's electronic brief of evidence for current court matters. The device will be pre-loaded with legally privileged material that has been provided by the inmate's legal practitioner (if they are represented) or the prosecuting authority if they are self-represented.

If an inmate's legal practitioner or prosecuting authority requires additional legal material to be uploaded to the device, they must notify JustConnect who will arrange for the device to be updated.

Inmates must be permitted to bring approved, Just Connect issued laptops or tablets (containing legal brief) to court when requested by the inmate or their legal team to assist them during a Court or AVL Court appearance. The request must be approved by the Governor (or Authorised officer) of the Correctional Centre.

Inmates are permitted to charge their approved laptops within their cells. However, inmates **are not permitted** to charge their approved tablets in their cells. These must be submitted to an accommodation officer who will be responsible for charging the tablet at the officer's station. An inmate must collect the charged tablet prior to lock-in.

All chargers, except for those in the High Risk Management Correctional Centre (HRMCC) must be contained in an approved secure box to prevent inmate access or tampering.

2.5 Inmate access to approved laptops or tablets issued by prosecuting authority (legal brief)

Inmates may be given access a laptop that will include their pre-loaded legal materials issued by the prosecuting authority (e.g. the Australian Federal Police)

Laptops issued by prosecuting authorities are not subject to approvals from the e-Brief Committee.

These laptop devices may have:

- Microsoft Office suite applications (MS Word and MS Excel) installed
- an embedded operational battery and
- requirements of a USB C laptop charging cable.

Upon receipt of the laptop, the inmate must:

- read and sign the *Waiver and release from liability* form and comply with all conditions
- only use the device while in their cell
- ensure that no other inmate has possession of, or uses, the device.

CSNSW retains the right to remove an approved laptop from an inmate's possession at any time for reasons such as suspected breach of the *Guidelines for inmate access to computer*, breach of security or misuse.

Content on an approved laptop is restricted to the inmate's electronic brief of evidence for current court matters. The device will be pre-loaded with legally privileged material that has been provided by the prosecuting authority.

If a prosecuting authority requires additional legal material to be uploaded to the device, they must notify Access to Justice who will arrange for the device to be updated.

Inmates must be permitted to bring approved Access to Justice issued laptop (containing legal briefs) to court when requested by the inmate or their legal team to assist them during a Court or AVL Court appearance. The request must be approved by the Governor (or Authorised officer) of the Correctional Centre.

Laptops provided by prosecuting authorities are supplied with a USB-C charging device. This device must be listed on the inmate's property as an "in cell laptop power source" to mitigate the risk of being charged with possession or use of a mobile phone. This is also recorded by the Access to Justice Team and the inmate will sign acknowledgment of receiving this item (along with the laptop). The Access to Justice Project Officer will liaise with the Governor (or authorised officer) where the inmate is housed to advise that the device and associated equipment is approved for the inmate's use.

2.6 Escalating issues or concerns relating to laptops or tablets containing legal briefs

Any issues or concerns arising from inmate access to computers issued by CSNSW or by a prosecuting authority must be reported by staff to the Governor/MOS, who may then raise the issue with Sentence Management.

	Procedure	**Responsibility**
1.	Raise any concerns regarding computers issued by prosecuting authority with Governor/MOS.	All staff
2.	Evaluate concerns raised, and either: • deal with concerns locally if possible, or • escalate concerns with Sentence Management by emailing to accesstojustice@dcj.nsw.gov.au.	Governor/MOS or authorised officer

3 Supervision

3.1 Policy

CSNSW staff must monitor inmate access to computers by regular supervision, Closed Circuit Television (CCTV) or by shadowing an inmate's green OAC computer session. Instructions on shadowing can be found in the OAC Manual (available at D17/289587 in EDRMS).

For computers located in Education areas, the supervising officer will be the Education Services Coordinator (ESC) or Assessment and Planning Officer (APO).

For computers located in Industries, the supervising officer will be the Industries Manager, Senior Overseer (SOS) or Overseer (OS).

Computers located outside of Industries or Education are the responsibility of custodial staff.

3.2 Procedures

When conducting regular supervision the supervising officer must:

	Procedure	Responsibility
1.	Check the cables connecting the computer to the network are connected to the correct computer and network ports.	Supervising officer
2.	Make sure inmates are only using the computer assigned to them.	Supervising officer
3.	Ensure that the inmate is logging in using the correct student/inmate login.	Supervising officer
4.	Make sure inmates are not attempting to tamper with the computer/software/hardware or cabling.	Supervising officer
5.	Regularly undertake a physical check of computer hardware for signs of tampering and submit a report if any is detected.	Supervising officer

3.3 Electronic supervision

Electronic supervision refers to checking computer drives, common drives and inmate files (inmate folders on the computer system) for non-authorised files and software. Green computers have a shadowing function allowing a supervising officer to follow an inmate's use in real time.

	Procedure	Responsibility
1.	Conduct and document monthly Computer Security Check and file in EDRMS.	Supervising officer
2.	When shadowing an inmate, avoid reading any documentation that relates to an inmate's legal proceedings as this information may be attract legal privilege.	Supervising officer

	Procedure	Responsibility
3.	Report any breach of protocol to the MOS or Governor immediately.	Supervising officer

4 Printing

4.1 Printing from inmate computers

Printing documents from inmate computers may be facilitated if centre operations provide for this. Inmates are required to pay for all personal printing and copying as per the library printing policy (refer to **COPP section *8.4 Inmate libraries***).

An inmate must not be seated near networked printers or permitted to use networked printers if they are not directly supervised by an officer. Each time an inmate begins a computer session all cabling into network printers must be checked to make sure they are connected to the correct port. The cabling must also be checked at the end of each session.

Red and green computers are connected to standalone printers that are separate from the OAC network. In some instances, a green computer using Pronto will be connected to a networked printer but the only printing available is from Pronto.

Printing from green computers must be directly related to education or employment.

Printing from red computers must be for the direct purpose of CSI employment.

	Procedure	Responsibility
1.	Check red computers, cabling and peripherals prior to an inmate accessing printers.	Supervising officer
2.	Supervise all printing.	Supervising officer
3.	Check red computers, cabling and peripherals at the cessation of duty.	Supervising officer
4.	Report any breach of protocol to the MOS or Governor immediately.	Supervising officer

4.2 Printing from the Legal Information Portal

The Library Liaison Officer will make available to inmates hard copies of forms and other information available on the Legal Information Portal.

4.3 Printing documents prepared by inmates for legal purposes

Documents prepared on blue computers by inmates for their legal purposes are not permitted to be printed by CSNSW staff. Refer to **COPP Section *20.8 Access to legal resources and to legal documents in storage*** for further information.

Documents prepared on OAC green computers by inmates for their legal purposes may be printed by the Library Liaison Officer at a cost to the inmate. Refer to **COPP Section *8.4 Inmate Libraries*** for further information.

5 Software

5.1 Policy

Approved software required by inmates may be installed on red or green inmate computers. Software must be approved by the Governor and installed on the OAC by Digital and Technology Services (DTS).

Inmate software is not permitted to be installed on blue computers.

The Education Services Coordinator is responsible for arranging the approval and purchase of education software and liaison with DTS. The inmate must meet the cost of software required for study purposes.

The Industries Manager (or representative) is responsible for arranging approval and installation of software required for employment purposes. The business unit must meet the cost of software required for employment purposes.

Software is not permitted to be kept by the inmate in their cell. The software user manual may be kept in the inmate's cell if it is recorded on the inmate cell property card. *COPP Section 4 Inmate property* will apply in terms of the amount of software inmates may keep on their property.

5.2 Inmate software register

The Industries Manager or Education Services Coordinator must maintain an *Inmate Software Register* for software installed on inmate computers.

The *Inmate Software Register* must record:

- the name and licence details of the software
- the name and Master Index Number (MIN) of the inmate who requires access to the software
- the name of the approver and date of approval
- the date the request to upload the OAC was submitted to DTS
- the date the software was installed on the OAC.

A monthly check of installed software must be recorded in the *Inmate Computer Security Check.*

6 Storage devices and transfer of data

6.1 Policy

An authorised officer can use a single-use external storage device to transfer data between corporate computers and inmate computers only for the direct purpose of inmate participation in education, programs or employment.

Under no circumstances must corporate data containing personal details of inmates or staff be transferred from corporate computers to inmate computers.

The transfer of data to external storage devices must be done by an authorised officer using a staff/administration log in.

Under no circumstances are inmates to be in the possession of an external storage device outside the work or education facility. Inmates found to be in possession of such devices will be charged with a correctional centre offence.

External storage devices used for the purpose of transferring data between corporate computers and inmate computers must only be used for the purpose of data transfer and must be reviewed on a monthly basis using the *Inmate Computer Security Check* and reported via the *Inmate Computer Check Report* (annexure on the last page of the *Inmate Computer Security Check*).

6.2 Register of external storage devices

A register of external storage devices used for transferring data between corporate computers for education purposes must be maintained by the Education Services Coordinator.

A register of external storage devices used for transferring data between corporate computers for employment purposes must be maintained by the Industries Manager.

A register of external storage devices used for transferring data between corporate computers and inmate computers or hard drives for legal purposes must be maintained by a designated officer appointed by the Governor or MOS.

6.3 Transfer of data for distance/external education programs

An authorised officer may transfer data for the purpose of study to an inmate personal folder on OAC green computers. The data must be removed from the inmate personal folder on OAC green computers on completion of the study.

If an inmate requires course material to be sourced from an external education service provider student portal or an external storage device:

	Procedure	Responsibility
1.	Access and download the course material to a corporate computer.	ESC
2.	Save the course materials to an external storage device.	ESC
3.	Transfer the learning materials to the OAC inmate personal folder.	ESC
4.	Record a case note detailing the course materials transferred to the OAC inmate personal folder.	ESC

An authorised officer may download data from an inmate personal folder on OAC green computers for submission to the external education provider.

If an inmate needs to submit documents to an external education provider:

	Procedure	Responsibility
1.	Transfer documents from the inmate's OAC personal folder to a corporate computer via an external storage device.	ESC
2.	Submit the documents to the distance learning institute via the inmate's student portal.	ESC
3.	Save a copy of the documents on the inmate's EDRMS student education file.	ESC
4.	Record a case note on OIMS detailing the submission.	ESC

7 Reporting infringements

Infringements of this policy and/or breaches of the *Guidelines for Inmate Access to Computers* must be reported immediately to the Manager of Security.

	Procedure	Responsibility
1.	Report any infringement or non-compliance of this policy.	All CSNSW staff
2.	Withdraw access to computers if an inmate is found to be in breach of the *Guidelines for Inmate Access to Computers* or poses other security risks.	MOS/FM
3.	Enter an alert in OIMS to indicate the access to computers has been withdrawn.	Authorised officer
4.	Determine if and when computer privileges may be reinstated.	Governor

8 Quick links

- *Related COPP*
- *Forms and annexures*
- *Related documents*

9 Definitions

APO	Assessment and Planning Officer
Authorised officer	The officer authorised by the Governor to perform the functions prescribed as part of the Custodial Operations Policy and Procedures
Blue Computers	Computers that are non-networked and are for the purpose of viewing and preparing legal documents

CCTV	Closed circuit television
CIG	Corrections Intelligence Group
Computers	Includes desktop, tablets, integrated television and laptop computers
CSI	Corrective Services Industries
CSNSW	Corrective Services New South Wales
DTS	Digital and Technology Services
ESC	Education Services Coordinator
FM	Functional Manager
Governor	Includes a Manager of Security in charge of a correctional centre.
Green Computers	Computers connected to the Offender Access to Computer network for the purposes of education, programs and employment
HRMCC	High Risk Management Correctional Centre
MIN	Master Index Number
MOS	Manager of Security
OS	Overseer
Red Computers	Computers that are non-networked and are for CSI employment purposes. Inmates must be approved to use red computers.

10 Document information

Business centre:		Custodial Operations
Approver:		Kevin Corcoran
Date of effect:		*16 December 2018*
EDRMS container:		*18/7205*
Version	**Date**	**Reason for amendment**
1.0		Initial publication *(Replaces section 5.4 of the superseded Operations Procedures Manual).*
1.1	12/03/20	General formatting update and improvements.
1.2	28/09/20	Policy reviewed and amended to include improved formatting, updated procedures and increased security measures. See ACCC Memorandum 2020/22 Revised COPP section 8.3 Inmate computers for further details.
1.3	04/05/23	Addition to subsection 2.4 to allow inmates to bring their Just Connect issued laptops to Court on application.
1.4	18/10/23	Addition of subsections 2.5 and 2.6 regarding computers issued by prosecuting authorities. See joint DC Memorandum 2023/*36 Inmate E-Brief Laptops (formerly Just CONNECT issued laptops)* for further details.