Justice Health and
Forensic Mental Health Network

Justice Health NSW Policy

Use of ICT Resources by Patients – Forensic Hospital

Issue Date: 03 August 2023

Together for
Healthier Tomorrows

Use of ICT Resources by Patients – Forensic Hospital

Policy Number 2.001

Policy Function Leadership and Management

Issue Date 03 August 2023

Next Review Date 03 August 2026

Risk Rating

Summary Within the Forensic Hospital, a range of programs has been developed to provide therapy, education and vocational training to patients using the computer medium.

This policy provides guidelines for access to computers by patients of the Forensic Hospital for the purposes of therapy, education, vocational training, as well as for research and the review of legal transcripts in relation to Court, trial and appeal matters.

Responsible Officer Executive Director Clinical Operations

Applies to
☒ Administration Centres
☐ Community Sites and programs
☐ Health Centres - Adult Correctional Centres or Police Cells
☐ Health Centres - Youth Justice Centres
☐ Long Bay Hospital
☒ Forensic Hospital
Other: (free text section to describe where/who the document applies to; if document only applies to certain area of a facility then describe here; if all staff are subject to the document then include this here).

CM Reference POLJH/0000

Change summary
- Transfer of existing policy to new template
- Updated all references and links to policies, guidelines, legislations, procedures, and forms.
- Added reference to NSW Cyber Security policy
- Added additional governance item under

Authorised by Chair, Policy Steering Committee

Revision History

#	Issue Date	Number and Name	Change Summary
1	May 2023	DG44168/23 Romen Hoque	• Transferred existing Policy to new Template. • Updated all references/links to policies, guidelines, legislations, procedures and forms.

			• Added references to NSW Cyber Security Policy. • Added governance item under 3.2
	June 2023	DG44168/23 Romen Hoque	• Updated acronym from JHNSW to Justice Health NSW • Added reference to guidelines instead of procedures • Updated minor formatting and recommendations

Justice Health and Forensic Mental Health Network
PO BOX 150 Matraville NSW 2036
Tel (02) 9700 3000
http://www.justicehealth.nsw.gov.au

1. Table of Contents

2. Preface

This policy provides guidelines for access to electronic devices by patients of the Forensic Hospital (FH) for the purposes of recovery, therapy, education and vocational training, as well as for research and the review of legal transcripts in relation to Court, trial and appeal matters.

The objectives of this policy are:

- To acknowledge the benefits to patients of access to computers, whilst also developing a structured framework that manages security compliance.
- To consolidate consistency of access to Information and Communications Technology (ICT) resources for all patients, subject to adherence to the approval process (refer to section 3.3) and the allocation of an appropriate Security Category and Leave Entitlement (SCALE) rating. Refer to policy 1.249 Leave, Ground Access and SCALE – Forensic Hospital.
- To detail Justice Health and Forensic Mental Health Network (Justice Health NSW) staff responsibilities for the security, storage and audit of all therapeutic, educational, vocational, legal research-related hardware and software held within the FH.
- To set out guidelines for patients to:
    - apply for approval to access ICT resources, via the stand-alone Forensic Hospital Patient Computer Network (FHPCN);
    - apply for approval to purchase software, ensuring compatibility with ICT infrastructure; and
    - request Justice Health NSW staff to transfer data by removable media for therapeutic needs and between the FH and a distance learning institutions.
- To implement clear guidelines which will ensure that all patients wishing to access ICT resources can be referred, assessed and enrolled in programs.
- To ensure that patient access to computers is strictly managed by means of an ICT infrastructure (FHPCN) designed to protect the Justice Health NSW physical and ICT security environment.

This policy applies to those ICT resources within the FH, **which are provided specifically and solely for patient recovery programs**, except when staff access a computer for the purpose of display only (Refer to section 3.3, point 3):

- eight student desktop computers including one teacher computer (which can be converted for temporary student login) in the FH Computer Training Room 1 in the Allied Health Hub, hereafter the Computer Training Room.
- printers, keyboards and mice;
- software provided by the FH for specific program use; and
- removable media such as CDs and DVDs.

3. Policy Content

3.1 Roles and Responsibilities

Manager Allied Health (MAH) and Chief Information Officer, ICT (CIO) or delegates are responsible for:

- the provision of computers and appropriate and compliant software. The purchase of these will be subject to normal Justice Health NSW procedures/guidelines and must be requested and purchased via ICT to ensure compatibility and alignment with Justice Health NSW policy 2.022 Delegations Authority; and
- ensuring that computers used by patients do not contain, are not connected to, nor have the facility to be connected to any internal or external communication device (such as a modem, USB etc.).

Manager Allied Health (MAH)/delegate is responsible for the compliance by all relevant staff and patients with the requirements of the Computer Training Room operational procedure. In particular, they:

- must ensure that physical supervision is provided by a minimum of two clinicians when patients are using computers in the Computer Training Room;
- must ensure that patients are not permitted to use the keyboard or mouse on any computer that is directly or indirectly linked to any Justice Health NSW system or network, or to the internet, (noting that patient access is allowed to the authorised and monitored stand-alone FHPCN, which is not connected to the Justice Health NSW system or the internet) [Note: staff are permitted to give therapeutic presentations to patients, including from the internet, provided that the prohibition on patient use of the keyboard and mouse is observed];
- must ensure that patients are not permitted access to information technology peripheral devices, including scanners, digital cameras, CD writers and other removable storage devices, such as USB sticks;
- are responsible for software storage and licence management;
- are responsible for enforcing the prohibition on the removal of computers from the Computer Training Room;

must ensure the maintenance and auditing of an accurate inventory of suitable hardware.
CIO/delegate is responsible for ensuring the continued operation of the FHPCN and all related ICT functions. In particular, they:

- are responsible for software distribution, which is centralised within the ICT department with installation occurring by remote connection on a schedule mutually agreed by ICT staff and the relevant clinicians; and
- are responsible for ensuring that antivirus protection software is in place, noting that patient computers are not updated for antivirus or security protection, as they are not connected to the Justice Health NSW network or the internet.

Nursing Unit Manager (NUM)/Nurse in Charge (NiC) Austinmer is responsible for:

- ensuring full compliance with patient computer usage on the unit, in particular with section 3.5.

Manager Security and Fire Safety (MSFS) is responsible for operational security, in consultation with the CIO and the MAH or delegates. In particular, they:

- must ensure that the Computer Training Room does not contain access to an external telephone connection, although a telephone with an internal access function only will be provided for staff security purposes.

Nursing Unit Managers, Forensic Hospital (NUM), After Hours Nurse Manager and Manager Allied Health (MAH) are responsible for approving access for removable media such as USBs, CDs and DVDs into the FH as per FH Procedure Prohibited and Controlled Items

3.2 Mandatory Requirements

This policy must be implemented by all staff and patients and applies to all senior managers, Nursing Unit Managers (NUMs), nursing, allied health and medical clinicians, other program staff and all staff who may be working in the Computer Training Room and/or supervising the use of the laptop in the Adolescent Unit, where therapeutic, educational, vocational and legal research programs are operating.

Patients are expressly prohibited from accessing the internet under any circumstances and by any means; this includes a complete prohibition on staff using their own Justice Health NSW login to allow patients to access the internet.

However, staff may use computers, including the internet, **in the presence of** patients to display presentations including power point presentations, videos, TAFE sites and psychological tools; staff facilitating such sessions must not permit patients to access the keyboard or mouse under any circumstances.

All items acquired for patient ICT programs must comply with FH Procedure Prohibited and Controlled Items – Forensic Hospital and Justice Health NSW policy 5.002 Access to the Forensic Hospital.

Governance
An agenda item added to Forensic Hospital Digital Health Committee (FHDHC) which is held monthly to discuss any risks or emerging risks due to Patient's access to technology across Forensic Hospital. Any identified risks will be captured and communicated to FH Senior Management for action and escalation (if required).

3.3 Patient Access

Patient access to computers occurs only in the following ways:

1. Direct access: individual or group access in the centralised Computer Training Room in the Allied Health Hub, directly supervised by at least two staff and with no internet access.
2. Supervised use of laptops in the Adolescent Unit, as detailed in section 3.4.2.
3. Staff usage of computers including the internet **in the presence of** patients to display presentations.

All patients seeking access to the Computer Training Room must undergo the approval process as follows:

1. The Staff member recommends participation as part of the therapy program. If the patient has the required SCALE rating, the relevant therapist may use clinical judgement and knowledge of the patient to approve access in the first instance. If the therapist has any concerns about the patient and/or has not worked with the patient in other therapy programs, then the decision to approve participation must be referred to the MDT and the process detailed below in points 2 to 4 must be followed.
2. The patient's multidisciplinary team (MDT) reviews access during the clinical review meeting. Areas for consideration must include:
    a. historical and current risk factors,
    b. record of compliance under unit conditions,
    c. current program participation,
    d. demonstrated responsible use of ground leave,
    e. current mental state,
    f. cognitive strengths and limitations,
    g. current SCALE rating,
    h. aims of enrolment in ICT programs, and
    i. any patient-specific issues.

3. If the risk assessment indicates that the patient qualifies for inclusion in the ICT program which operates in the Computer Training Room, then an application for grounds access must be lodged detailing patient SCALE and time allowance recommendation (or confirmed where patient already has the required SCALE) and must be approved by the treating psychiatrist. The grounds application must be approved by the Forensic Hospital Leave Committee and must comply with all requirements of Justice Health NSW policy 1.249 Leave, Ground Access and SCALE – Forensic Hospital.
4. The outcome of the MDT review must be documented in the patient's health record. Therapy staff will inform the patient of the outcome and if s/he is successful, program time(s) are scheduled into the multidisciplinary timetable.
5. All leave must be preceded by a risk assessment on the day itself in compliance with Justice Health NSW policy 1.249 Leave, Ground Access and SCALE – Forensic Hospital.

3.4 Operating Procedure

3.4.1 Computer Training Room Procedure

- All procedures/guidelines in the Computer Training Room must comply with the Justice Health NSW security-related policies 5.002 Access to the Forensic Hospital, 5.005 Alarm, Pager & Two-Way Radio Use and Management – Forensic Hospital and 5.017 Management of Emergencies – Forensic Hospital.
- A minimum of two staff trained in Violence Prevention and Management (VPM) must remain in the room with the patient(s) throughout the therapy or training session to provide direct and constant physical supervision and to:
    - carry out a visual check of the room at the start and end of the session to ensure that no inappropriate or personal material has been left by any patient;
    - ensure that patients are only using the desktop computers assigned to them;
    - enter patients' names into the Patient Computer Use Register, together with the date and the number of their allocated computer;
    - ensure that patients are not engaging in inappropriate or illegal activities, such as accessing, viewing or storing pornographic, sexually explicit or otherwise inappropriate material or using prohibited peripheral devices; and
    - ensure that patients are not tampering with the desktop computer software or hardware.

  In addition to therapy/teaching staff leading the session, support may be provided by other allied health clinicians, allied health assistants, nursing staff or mental health care workers.

- All staff leading sessions in the Computer Training Room must be trained in the operation of the FHPCN.
- During the first session in the Computer Training Room, the following must occur:
    - orientation of the patient to the Computer Training Room and facilities, including toilet access;
    - demonstration of the correct posture, seating and alignment of the work station; and
    - assignment to each patient of an individual folder for storage of their data/documents.

  The patient must also confirm that s/he has agreed to abide by the rules and regulations of the Computer Training Room by signing Form JUS020.800 AGREEMENT Patient Use of ICT Resources - Forensic Hospital. Refusal to sign will result in termination of that patient's enrolment in the ICT program. This form must be filed in the patient's health record.

- Patients must log into the patient computers with generic accounts (student 1, 2 etc.) and save their data to a central server. The patient data (.doc, .xls etc.) saved on this server will be copied in full daily to an external storage device and overwritten as required. Once the data is overwritten, it cannot be restored – no historical data will be kept.

- At the end of each session, the therapist/teacher must transfer data from each generic student account into an individually named patient folder belonging to the corresponding student. This data can then be retrieved for the student in their next session and it is protected from viewing by other students.

- Patients may be studying through:
    - OTEN (Open Training and Education Network), a distance learning unit of TAFE NSW Western Sydney Institute; and/or
    - Sydney Distance Education High School which is a distance education provider.

For both these options, the provider has established an online site offering course information and student registration. The site is accessed on the patient's behalf, with their knowledge and permission, by the group facilitator, who then supplies hard copies to the patient. The provider sends USBs/CDs to Justice Health NSW which are installed remotely by ICT staff on a schedule mutually agreed by ICT staff and relevant clinicians. If the coursework requires students to complete an assignment, the supervising clinician should print out the student responses and mail a hard copy or email a scanned copy to the provider. Course notes from websites may also be copied onto CD as a collection of data in HTML format; these CDs are sent to the patient and may be stored with the patient's property, following approval by the NUM or MAH/delegate. The CDs may be interactive but must only be viewed by patients in the Computer Training Room where there is no internet connection/access.

Access to university and other educational programs may be established in the future, provided such access complies with the directives and requirements of this policy and all other related documents.

- An equipment register must be established for all devices such as mice, keyboards and other accessories. Registered items must be signed out at the beginning of each session and accounted for at the end.
- A clinician must directly supervise any patient using the colour printer and must ensure compliance with section 3.5.
- In the event of an emergency or aggressive incident, de-escalation techniques should be attempted in the first instance. In the case of injury or medical emergency, staff should administer first aid. In both instances, if required, personal duress alarms should be activated to summon the Emergency Response Team. Refer to Justice Health NSW policy 5.005 Alarm, Pager & Two-Way Radio Use and Management – Forensic Hospital & 5.017 Management of Emergencies – Forensic Hospital.
- A verbal handover must be provided to the patient's allocated nurse by the leading therapist/teacher and a report documented in the health record on the patient's return to their unit.
- All incidents must be logged on the Incident Information Management System (IIMS) in accord with Ministry of Health policy PD2020_047 Incident Management Policy.

3.4.2 Austinmer Adolescent Unit Procedure

A laptop computer (referred to in this section as "the laptop") supplied by the NSW Department of Education (DoE) will be used to provide education and training for young people resident in the adolescent unit **only**.

These sessions must comply with all relevant NSW Ministry of Health and JHNSW policies and procedures, and related legislation and must operate as follows:

- Training must be implemented by the DoE Assistant Principal/School teacher (AP/ST)AP/ST, or a delegate appointed by the MDT in the absence of an AP/ST only.
- A JHNSW staff member(s) must also be present, if indicated by a risk assessment, the student/patient's SCALE rating and the size and composition of the patient group in the room.
- Patients must be approved to attend by the MDT in accord with relevant assessment criteria (refer to section 3.3) and confirmed by the NUM or NiC on a sessional basis.
- During the first session the AP/ST must demonstrate the correct posture, seating and alignment to the work station to the patient. The patient must also confirm that s/he has agreed to the rules and regulations of the ICT program (refusal will result in termination of that patient's enrolment in the ICT program). This confirmation must be recorded by signing Form JUS020.800 A AGREEMENT Patient Use of ICT Resources - Forensic Hospital which must be filed in the patient's health record.
- The training must comprise word processing and access of educationally relevant software only.
- Each patient must access the laptop individually and must be directly supervised by the AP/ST at all times as well as supporting JHNSW staff.
- The laptop should only be used in areas of the adolescent unit which have no internet connection available. Network connections and the infra-red port should be disabled, wherever possible.
- There must be no data cable, peripheral devices or removable storage devices attached to the laptop or available for patient use. There must be no camera installed on the laptop; any camera contained in the laptop must be disabled.
- The AP/ST or a JHNSW staff member must directly supervise any patient using the colour printer and must ensure compliance with section 3.5.
- Patients must not be able to access the High Security Level Administrator settings on the laptop. They must have their own user setting to which they must not be given the password; patients must be logged in by the AP/ST prior to the patient's arrival for the session.
- All clinical interventions must be documented in the patient's health record and
- All incidents must be logged on the Incident Information Management System (IIMS) in accord with Ministry of Health policy PD2020_047 Incident Management Policy.
- When not in use, the laptops must be locked in the AP/ST's storage cupboard in the upstairs office area above the Austinmer unit.
- These procedures relate to the current laptops computers supplied by the NSW Department of Education (DoE), which may be replaced or upgraded as necessary. However, all the above procedures and prohibitions will still apply and must still be observed. Maintenance is the responsibility of DoE and there is to be no cost to JHNSW involved in either the purchase or maintenance.

3.5 Principles of Operation

3.5.1 Programming

Occupational and diversional therapists will be primarily responsible for the development of programs in the Computer Training Room under the supervision of the MAH and Senior Therapist.

3.5.2 Policy Breaches

- Supervising staff must report any infringement or non-compliance with this policy to the Director of Nursing and Services FH (DNS), the MAH, the CIO, the MSFS and, in the case of the Austinmer Adolescent Unit, the NUM or NiC as well.

- The following breaches will result in immediate withdrawal of the patient's computer access for a specified period to be determined by the MDT:
    - sending offensive messages and inappropriate images or other offensive material, which constitutes a form of harassment;
    - engaging in inappropriate or illegal activities, such as accessing, viewing or storing pornographic, sexually explicit or otherwise inappropriate material;
    - using prohibited peripheral devices; or
    - tampering with the computer software or hardware.

  Access will be reviewed by the MDT at the end of the exclusion period.

- Colour printing by patients of identity documents, such as drivers' licences, passports, student cards and academic or professional qualifications, must only be allowed for verified official purposes and must occur under direct staff supervision.
- Where continuing supervision cannot be provided in strict accordance with this policy, all patient access to the Computer Training Room and/or the laptop in the Adolescent Unit must be suspended immediately.

3.5.3 Legal Issues

Official Records

- Files created by patients when using the ICT resources do not constitute a record as defined in the Ministry of Health PD2009_076 Communications - Use & Management of Misuse of NSW Health Communications Systems. Therefore, there is no requirement to monitor use and record created files in Content Manager.
- Records of the nature and content of Justice Health NSW ICT resources constitute a Justice Health NSW record, which may be subject to the State Records Act 1998-017 and the Government Information (Public Access) Act 2009-052, as well as other laws concerning disclosure and privacy.

Breaches that Break the Law

Any suspected breach of this policy that would violate Commonwealth or State laws or regulations must be reported to the CIO and the DNS.

4. Definitions

Delegated officer/Delegate
In relation to a function, Delegated officer/Delegate refers to a staff member authorised by the responsible officer to exercise that function.

SCALE
Security Category and Leave Entitlement

FHPCN
Forensic Hospital Patient Computer Network

MDT
Multidisciplinary team

EPO
Education Project Officer

NUM
Nurse Unit Manager

NiC

Nurse in Charge

PAS
Patient Administration System

DE
Department of Education

FHDHC
Forensic Hospital Digital Health Committee

5. Related documents

Legislations	Anti-Discrimination Act 1977-048 Crimes Act 1900-040 Government Information (Public Access) Act 2009-052 Health Services Act 1997-154 Health Records and Information Privacy Act 2002-071 Independent Commission Against Corruption Act 1988-035 Mental Health Act 2007-008 Mental Health and Cognitive Impairment Forensic Provisions Act 2020-012 Privacy and Personal Information Protection Act 1998-133 State Records Act 1998-017 Telecommunications (Interception and Access) (New South Wales) Act 1987 No 290 Work Health and Safety Act 2011 No 10 Workplace Surveillance Act 2005 No 47
Justice Health NSW Policies, Guidelines and Procedures	1.078 *Care Coordination, Risk Assessment, Planning and Review – Forensic Hospital* 1.249 *Leave, Ground Access and SCALE – Forensic Hospital* 2.002 *Acceptable Use of Communication Systems* 2.010 *Code of Conduct* 2.022 *Delegations Authority* 2.155 *Enterprise-Wide Risk Management* 5.017 *Management of Emergencies – Forensic Hospital* 5.110 *Work Health and Safety* Work Health and Safety Risk Management – Hazard Identification, Risk Assessment and Control PROCEDURE 5.135 *Security Risk Management* Prohibited and Controlled Items
Justice Health NSW Forms	Form JUS020.800 *AGREEMENT Patient Use of ICT Resources - Forensic Hospital*
NSW Health Policy Directives and Guidelines	PD2019_020 *Clinical Handover – Standard Key Principles* PD2009_076 *Communications - Use and Management of Misuse of NSW Health Communications Systems* PD2021_039 *Mental Health Clinical Documentation* PD2020_046 *Electronic Information Security Policy – NSW Health* PD2020_047 *Incident Management Policy* PD2015_049 *NSW Health Code of Conduct* IB2022_039 *Protecting People and Property: NSW Health Policy and Standards for Security Risk Management*

NSW Cyber Security Policy