Health
Justice Health &
Forensic Mental Health Network

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

Use of ICT Resources by Patients – Forensic Hospital

Policy Number 2.001

Policy Function Leadership and Management

Issue Date 28 September 2018

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 and 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

Applicable Sites

- ☒ Administration Centres
- ☐ Community Sites (e.g. Court Liaison Service, Community Integration Team, etc.)
- ☐ Health Centres (Adult Correctional Centres or Police Cells)
- ☐ Health Centres (Juvenile Justice Centres)
- ☐ Long Bay Hospital
- ☒ Forensic Hospital

Previous Issue(s) Policy 2.001 (Sept 2015; May 2014)

Change Summary

- Titles updated
- Related policies and procedures updated
- Sections related to unit-based computers deleted, as purchase has been deferred pending negotiation around internet access and resolution of associated security issues

TRIM Reference POLJH/2001

Authorised by Chief Executive, Justice Health and Forensic Mental Health Network

1. Preface

This policy provides guidelines for access to computers by patients of the Forensic Hospital (FH) for the purposes of 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 3.1) and the allocation of an appropriate *Security Category and Leave Entitlement* (SCALE) rating. Refer to JH&FMHN policy 1.249 *Leave, Ground Access and SCALE – Forensic Hospital*.
- To detail Justice Health and Forensic Mental Health Network (JH&FMHN) staff responsibilities for the security, storage and audit of all therapeutic, educational, vocational and legal research-related hardware and software held within the FH.
- To set out procedures 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 JH&FMHN staff to transfer data by removable media for therapeutic needs and between the FH and a distance learning institution.
- To implement clear procedures 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 JH&FMHN physical and ICT security environment.

This policy applies to those ICT resources within the FH, **which are provided specifically and solely for patient programs**, except when staff access a computer for the purpose of display only (Refer to section 3.1, 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.

2. Policy Content

2.1 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 JH&FMHN 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 Powerpoint, 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* and JH&FMHN policy 5.002 *Access to the Forensic Hospital*.

2.2 Implementation - Roles & 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 JH&FMHN procedures and must be requested and purchased via ICT to ensure compatibility and alignment with JH&FMHN 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 stick 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, s/he:

- 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 JH&FMHN 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 JH&FMHN 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;
- is responsible for software storage and licence management;
- is responsible for enforcing the prohibition on the removal of computers from the Computer Training Room;

- must ensure that audits of the patients' stored data are performed regularly to detect any breach of protocol;
- is responsible for assessing and approving the storage of individual patient CDs in the patient's property; and
- ensuring the maintenance and audit of an accurate inventory of suitable hardware. The inventory must contain the following information:
    - asset number,
    - serial number of the computer,
    - make and model of the computer, and
    - component details:
        a) type of processor.
        b) memory size.
        c) hard disk size and serial number.

CIO/delegate is responsible for ensuring the continued operation of the FHPCN and all related ICT functions. In particular, s/he:

- is 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
- is 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 JHFMHN network or the internet..

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

- ensuring full compliance with patient computer usage on the unit, in particular with section 3.3.

Nursing Unit Manager (NUM)/Nurse in Charge (NiC) Austinmer Women's, Bronte, Clovelly, Dee Why and Elouera Units are responsible for:

- ensuring full compliance with patient computer usage on their own units.

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

- 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) and Manager Allied Health (MAH) are responsible for approving access for removable media such as USBs, CDs and DVDs into the FH.

3. Procedure Content

3.1 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 the laptop in the Adolescent Unit, as detailed in section 3.2.3.
3. Staff usage of computers including the internet **in the presence of** patients to display presentations. Patients are **not** permitted to access the keyboard or mouse under any circumstances.

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

1. The therapist 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 JH&FMHN 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 JH&FMHN policy 1.249 *Leave, Ground Access and SCALE – Forensic Hospital*.

3.2 Operating Procedures

3.2.1 Computer Training Room Procedure

- All procedures in the Computer Training Room must comply with the JH&FMHN 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 JH&FMHN 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 3.3.
- 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 JH&FMHN policy 5.005 *Alarm, Pager & Two-Way Radio Use and Management – Forensic Hospital* & FH Procedure *Medical Emergencies - Management.*
- 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 clinical interventions must be documented in the patient's health record and should also be logged on the Patient Administration System (PAS).
- All incidents must be logged on the *Incident Information Management System* (IIMS) in accord with Ministry of Health policy PD2014_004 *Incident Management Policy*.

3.2.3 Austinmer Adolescent Unit Procedure

A laptop computer (referred to in this section as "the laptop") supplied by the NSW Department of Education (DE) 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 JH&FMHN policies and procedures, and related legislation and must operate as follows:

- Training must be implemented by the DE Education Project Officer (EPO) FH, or a delegate appointed by the MDT in the absence of an EPO only.

- A JH&FMHN 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 3.1) and confirmed by the NUM or NiC on a sessional basis.
- During the first session the EPO 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 *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.
- Patients must access the laptop individually and must be directly supervised by the EPO at all times. No other patients must be permitted within close proximity of the laptop.
- 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 EPO or a JH&FMHN staff member must directly supervise any patient using the colour printer and must ensure compliance with section 3.3.
- 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 EPO prior to the patient's arrival for the session.
- The EPO must check the patient's work and stored data both throughout and on completion of the session. Patient work must be downloaded and printed by the EPO or sent directly to distance education providers from the EPO's computer in their office area.
- The patient's allocated nurse must obtain a verbal handover from the EPO and document that report in the patient's health record.
- All clinical interventions must be documented in the patient's health record and logged on the Patient Administration System (PAS).
- All incidents must be logged on the *Incident Information Management System* (IIMS) in accord with Ministry of Health policy PD2014_004 *Incident Management Policy*.
- When not in use, the laptop must be locked in the EPO's storage cupboard in the upstairs office area above the Austinmer unit.
- These procedures relate to the current laptop computer supplied by the NSW Department of Education (DE), 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 DE and there is to be no cost to JH&FMHN involved in either the purchase or maintenance.

3.3 Principles of Operation

3.3.1 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.

3.3.2 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.

3.3.3 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 HPRM.
- Records of the nature and content of JH&FMHN ICT resources constitute a JH&FMHN record, which may be subject to the *State Records Act 1998* and the *Government Information (Public Access) Act 2009*, 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.

Must

Indicates a mandatory action or requirement.

Should

Indicates a recommended action that needs to be followed unless there are sound reasons for taking a different course of action.

5. Legislation and Related Documents

Legislation	*Anti-Discrimination Act 1977* *Crimes Act 1900* *Government Information (Public Access) Act 2009* *Health Services Act 1997* *Health Records and Information Privacy Act 2002* *Independent Commission Against Corruption Act 1988* *Mental Health Act 2007* *Mental Health (Forensic Provisions) Act 1990* *Privacy and Personal Information Protection Act 1998* *State Records Act 1998* *Telecommunications (Interception and Access) Act 1979* *Work Health and Safety Act 2011* *Workplace Surveillance Act 2005*
NSW Ministry of Health Policy Directives and Information Bulletin	PD2009_060 *Clinical Handover – Standard Key Principles* PD2009_076 *Communications - Use and Management of Misuse of NSW Health Communications Systems* PD2010_018 *Mental Health Clinical Documentation* PD2013_033 *Electronic Information Security Policy – NSW Health* PD2014_004 *Incident Management Policy* PD2015_049 *NSW Health Code of Conduct* IB2013_024 *Protecting People and Property: NSW Health Policy and Standards*

	for Security Risk Management
JH&FMHN Policy	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* 5.115 *Work Health and Safety Risk Management (OHS Hazard Management)* 5.135 *Security Risk Management* FH Procedure *Medical Emergencies - Management* FH Procedure *Prohibited and Controlled Items*
State Records NSW	*Policy on Electronic Messages as Records (Issued 1998)* *Policy on Electronic Recordkeeping (Issued 1998)*