Title:	**ICT Network Access**
Document type:	**Policy**

BRHS
Bairnsdale Regional Health Service

PURPOSE:
The purpose of this Policy is to outline Bairnsdale Regional Health Services' (BRHS) approach to the use of BRHS network.

POLICY:
BRHS staff must only access the BRHS network using a BRHS allocated username and password, see User account and password policy. The level of access to the Network will be determined by job role.

Every BRHS staff member shares the obligation to preserve the security and privacy of BRHS systems accessed from the BRHS network.

BRHS ICT Staff are the only employees authorised to load computer programs onto the BRHS network.

The BRHS network must not be used to download large files, such as books, movies or software, for personal use.

Downloading or playing electronic games on the BRHS network is forbidden.

The BRHS's network must not be used to access, store or transfer material, such as pornography, pirated software, pirated movies or pirated music.

Privately owned devices may be connected to the BRHS network only via a wireless connection.

- BRHS reserves the right to inspect all privately owned devices which are connected to the BRHS network to investigate suspected security breaches, inappropriate or illegal activity, or unauthorised access.
- BRHS reserves the right to subject privately owned devices to a process of certification before the device will be allowed to operate on the network.
- BRHS accepts no responsibility for any loss or damage to either the physical device or data contained within it as a result of connecting it to the BRHS network.
- BRHS accepts no responsibility for the support and maintenance of privately owned devices whether or not they are used for BRHS business.
- With the exception of data storage media, privately owned devices may not be connected as peripherals to BRHS owned workstations or servers without explicit permission from the ICT Manager.
- The connection of data storage media to staff workstations is permitted but BRHS does not guarantee compatibility support for such equipment.
- Storing of corporate information on privately owned equipment is only permitted if:
    - The privately owned equipment is suitably secured as warranted by the confidentially, privacy and integrity of the information in question.
    - Any suspected loss or breach of security with respect to BRHS corporate information is immediately reported to ICT Manager.
- By connecting a private machine to the intranet/BRHS network a user has acknowledged that they will be bound by the BRHS conditions of use of information technology services.

BRHS respects the rights of staff using the network for valid work purposes. However, where there is abuse, or suspected abuse, of the network or network services, BRHS has the right to inspect individual workstations

The hard copy of this document may be out of date. To ensure you are reading the current version, check the policy and guideline site on the BRHS Intranet.

and servers, along with the contents of all files, messages and logs contained on those machines and servers, and make whatever correlation is required to investigate such abuse or suspected abuse.

With respect to Wireless Network Access, BRHS designates the following individuals as BRHS guests:

- Vendors and consultants executing existing BRHS contracts
- Presenters, visiting specialists, and speakers facilitating BRHS-sponsored events
- Patients, patient visitors and the general public.

BRHS guests must connect to the guest wireless network through authentication of assigned credentials. Credentials are provided by the IT Helpdesk after review and approval.

BRHS reserves the right to quarantine, suspend, or otherwise disable network access to staff or guest owned devices found to pose a threat to network security with or without prior warning or consent.

EVALUATION:
Network monitoring tools will be used to monitor network access.

KEY WORDS:
Network, computer, guest, wireless, devices

ASSOCIATED DOCUMENTATION:
User Account and Password Policy

KEY LEGISLATION, ACTS and STANDARDS:
N/A

REFERENCES:

STAFF CONSULTED IN DEVELOPMENT / REVIEW:
* Denotes author

Name	Position	Service / Program
*Daniel Whittingham	ICT Systems Analyst Lead	Information Communications & Technology
Bill Morfis	Director	Corporate Services
Endorsed by Committee **Date:** **Agenda Number:**	Information Management committee 27 April 2022 5.6	
Approved by Committee **Date:** **Item Number:**	Executive Governance Committee 17 May 2022 8.5.3	

The hard copy of this document may be out of date. To ensure you are reading the current version, check the policy and guideline site on the BRHS Intranet.

Is this a new or revised document?	New document/s: Provide a rationale as to why it is needed. Revised document/s: Please details or highlight the changes, include title changes	New ☐ Revised ☒
Change description	Provide a brief summary of the changes to enable this to be communicated to staff	Update to new format only

Document Management
Policy supported:
Executive Sponsor: Director Corporate Services
Person Responsible: Manager ICT & Systems

Previously consulted in the development / review of this document:

AUTHOR/CIRCULATION:

* Denotes author

Name	**Position**	**Service / Program**
* Peter Binding	ICT Manager	Information Communications Technology
Therese Tierney	Chief Executive Officer	

COMMITTEE FOR ENDORSEMENT: Information Management Committee members

DEFINITIONS:

Word	**Definition**
ICT	Information & Communications Technology

Approved By: Chief Executive Officer

The hard copy of this document may be out of date. To ensure you are reading the current version, check the policy and guideline site on the BRHS Intranet.