BHI - Mobile Devices Policy
Version 1.0

Authorised by: CEO **Endorsed By:** Chief Operations Officer

Document: BHI - Mobile Devices Policy

Document No.: ITS-POL-003

Process Area: Technology Solutions

1 Document Control

Version	Date	Amended by	Changes Made
0.1	20/01/2017	Lars Cortsen	Initial document
0.2	29/03/2017	Simon Hahnel	Incorporate TS Team Feedback
1.0	14/04/2017	Simon Hahnel	Executive Feedback and Approval
	17/05/2019	Academic Quality Assurance Officer	Minor administrative changes to remove reference to 'BHIG' and 'CAE'

2 Purpose

The purpose of this policy is to provide appropriate guidelines, so that BHI employees, Students, third party contractors and suppliers can use Mobile Devices (defined as including but not limited to the following: laptops, netbooks, MAC's or similar mobile PC's, Android devices (Google, Samsung, Sony etc..), iOS devices (iPhones, iPads), tablets, Wireless dongles/modems (3-4-5G or similar/future mobile technology) with or without cellular capability) to connect to, and access BHI data residing on BHI network(s).

This Policy also addresses the procurement, management and support of all Mobile Devices to ensure proper control, while providing employees flexibility to choose their Mobile Device without sacrificing BHI's ability to manage and support these devices.

This policy also describes associated security requirements and employee's responsibility for appropriate use of mobile devices.

3 Scope

This policy applies to anyone accessing BHI's network or accessing BHI data, such as employees, students, third parties, contract workers etc.

It also applies to anyone who wishes to use a BHI or a personally owned mobile device (also known as BYOD – **B**ring **Y**our **O**wn **D**evice) connecting to BHI's networks and data.

4 Policy Statement

4.1 Procurement guidelines

For a current list of approved devices (BHI owned and provided) refer to the latest "mobile device procurement procedure" specifying the specific mobile phones and tablets available and used at BHI. These can always be requested via a formal request to BHI IT Support Team.

4.2 Personally Owned Devices

Employees, Students or contractors may connect their personal mobile devices to the BHI's network to access, download and manage BHI data, provided their mobile device meets the minimum security and management standard set by BHI IT.

To connect a “Bring Your Own Device” (BYOD) to BHI’s corporate network a user must submit a service request to the BHI IT Service Team, in order to get their mobile device connected to BHI’s corporate network.

Anyone wishing to access BHI’s corporate network may be required to sign an agreement allowing BHI to wipe any device using to access BHIs corporate network, or any device that contains BHI data in the event their employment or contract (Students or contractors etc.) is terminated or ends or if the device is or suspected to be lost or stolen.

All BYOD users must comply with the “BHI Code of Conduct” at all times.

Applications that are not provided by a legitimate source, are not permitted under any circumstances. Examples of legitimate application are iTunes or Google Play

If exceptions apply, the BYOD owner must get a written approval from BHI IT, by creating a service request with the BHI IT support Team.

BHI does not tolerate the use of any mobile device when driving. Hands free conversation is acceptable as defined by Victorian traffic law.

BHI does not undertake any liability for the employee’s personal data that may be stored on the users’ device. The device user undertakes responsibility for any loss of company/personal data due to errors, bugs, viruses, malware and other software or hardware issues that arise or any other errors that make the device unusable.

The BYOD user is personally liable for all costs associated with his/her own device.

BHI may disconnect or disable services provided without notifying the user if deemed necessary.

4.3 Students, visitors and public access

Student access to the BHI network is limited, but will allow all students to access data that is required to perform their Box Hill Institute studies.

Public access for BHI visitors to BHI provided Internet, can be accessed by accepting BHI’s public Terms and Conditions.

4.4 Reimbursement of cost for personally owned mobile devices

Users who wish to re-charge BHI for the cost of communications associated with a personally owned Mobile Device, which has been authorized to connect to the BHI corporate network must obtain approval from his/her department manager before such cost has occurred.

4.5 Lost, stolen or broken mobile devices (BHI owned and BYOD)

BHI will not be liable for any damage to or loss of employee owned mobile Devices. Employees who replace their personally owed mobile device, and want to connect a new personally owed device to BHI’s corporate network(s) must follow the process as described in this policy.

In the event a company or employee owned mobile Device that is connected to the BHI corporate network is lost, stolen or misplaced, BHI IT must be notified immediately through the BHI IT Service Team, so that appropriate steps can be taken to remotely delete the data contained on such device, or otherwise manage the increased risk for BHI’s network.

4.6 Configuration of a mobile device (BHI owned and BYOD)

BHI employees or third parties must not change any BHI configured security settings of the mobile device (except changing device passwords) after they have been configured by a BHI IT technician.

Before using a mobile device accessing BHI's corporate network, the BHI IT function must have configured the security settings as per the BHI IT Standard Operating Procedures (SOP).

4.7 Software of a mobile device (BHI owned and BYOD)

For ease of understanding this section is split into "laptops" and "other mobile devices"

4.7.1 Laptops and similar mobile PC's

All mobile PC's must have the following BHI approved software installed before accessing any part BHI's corporate network:

1. A BHI IT approved virus scanner software solution
2. A BHI IT approved firewall software solution

Furthermore, all mobile PC's must:

3. Be part of BHI's Active Directory (AD) domain to enable BHI Policies to be applied

4.7.2 Mobile devices excluding laptops/Netbooks and similar mobile PC's

All mobile devices accessing BHI's corporate network and data, but excluding mobile PC's must be managed by a BHI IT approved Mobile device management (MDM) platform

4.8 Acceptable use of a mobile device (BHI owned devices only)

Mobile service users are responsible to ensure the following:

- Ensure that proper care, use and maintenance of their mobile devices.
- That their mobile devices are kept securely and always utilise password access/protection.
- Ensure **personal** mobile service usage is kept at a absolutely minimum (Max $10 a month)
- BHI IT is advised of faults immediately for timely replacement/repair of the unit
- Advise BHI IT of loss or theft of any device to ensure the carrier is alerted immediately (by next working day at a minimum)

4.9 Physical security (any device that accesses BHI's corporate network)

Mobile service users are responsible to ensure that mobile computing devices:

- Are not left unattended visibly in a vehicle or in a public place
- Are properly secured when not on or with the individual

4.10 Mobile data protection

BHI IT must ensure that mobile computing devices are configured to ensure:

- Passwords or codes are required to access the device
- Data is encrypted on the device
- Use anti-malware software where possible
- Allow remote erase capability (for stolen mobile devices)

- The device must lock itself with a password/access code if left for more than 6 minutes.

Users are responsible for:

- Abide by the BHI corporate Network Security policies
- Not rely on mobile computing devices as the only repository of data
- Ensure all data is backed up to the BHI network
- Not alter any BHI mobile computing device without prior permission from IT
- Report any lost, damaged or stolen devices to the IT service hub BHI does not take responsibility for any personal information stored or managed on a mobile computing device in the event of loss or damage

4.11 Mobile connectivity

All users are expected to ensure that the mobile computing devices comply with the staff electronic communications policy as published by BHI

4.12 Termination of mobile service (BHI owned devices only)

The following are necessary for termination of mobile services:

- Where a mobile service is terminated, the SIM card and the mobile device, is to be returned to BHI IT within 24 hours, or by the next business day by the employee/user – whatever comes first.
- The direct supervisor of the employee must recover the mobile device and SIM card from the user where the user is no longer providing services to BHI. The direct supervisor must inform the Manager - Technology Solutions, that the device and SIM card has been recovered.
- When an employee is leaving BHI, IT will action the collection of any mobile device as authorised by the employee manager.
- When a mobile device has been lost, stolen, involved in a security breach, has had unacceptable usage, BHI IT may suspend the mobile device, and return it to its default settings.

4.13 Password requirements

The following requirements apply specifically to mobile devices (but excluding mobile PC's) to ensure proper passwords are used:

- BHI may audit the device to ensure users have password enabled.
- "Simple password" is disabled to prevent password like 1234, 1111 etc.
- Maximum failed login attempts before device is locked and/or wiped (depending on the device) will be set at 10 failed attempts.
- Recommendation to have maximum inactivity time lock at 10 minutes.

Please consult the generic BHI Password Policy as well.

All mobile PC's must follow the BHI Password Policy.

4.14 Generic Security requirements for all mobile devices

All mobile devices, without exception, must meet the following criteria before connection to BHI corporate network is permitted:

- Data traffic between any BHI's corporate network, and any mobile device should be encrypted
- BHI data stored on the mobile device should be encrypted, and password/login protected (see password requirements in section 4.13)
- BHI must have the ability and authority from the employee/user to remove any data (to include wiping the entire device (if required) from the mobile device at any time without prior Key user rules – a summery

Action	**Rule**
Usage of a mobile device – PC's included	- Report the loss or theft of devices. - Report any found device. - Report any unknown device. - Report the manipulation of devices. - Store the device in a safe place resp. take care of the device when you are on the way. - Never use non BHI provided or BYOD that's not approved and configured by BHI IT. - Back up the data regularly.
Configuration of a mobile device	- Do not change the security settings. - Have the security settings configured before using the device.
Software on a mobile device	- Use virus scanner software. - Use personal firewall software. - Use access control software. - Assign access rights. - Use encryption software where possible.

5 Code of Conduct

All employees are expected to conduct themselves in a manner consistent with the Box Hill Institute Code of Conduct for Employees.

6 Definitions

Term	Definition
Mobile Service	A company that offers mobile communication services to users of mobile devices such as smartphones and tablet PCs.
Service User	Individual accessing mobile services through a smartphone or device to complete their job/task.
Carrier	A telecommunications company that provides voice and telecommunication services.
Mobile Device	A small computing device, usually small enough to be handheld having a display screen with touch input and/or miniature keyboard.
Smart Device	An electronic device that is connected to other devices or networks via different wireless protocols.
SIM	(Subscriber identity/identification module) a removable card inside a cell phone that stores data unique to the user, as an identification number, phone numbers, passwords and message.
Corporate Network	BHI Network restricted to staff for corporate application access.
Student Network	BHI Network made available to all student and public guests for the distribution of BHI Learning Materials.
Public Network	BHI Network made available to corporate and convention centre guests.

7 Related Procedures

N/A

8 Related Operating Guidelines

N/A

9 Related Forms

N/A

10 Related Legislation and Registration

10.1 Box Hill Institute

10.2 External

Related Legislation and Registration

SEC POL 01 Information Security Management Policy, Victorian Government CIO Council, October 2012.

Victoria: Financial Management Act 1994

Victoria: Regulations to the Financial Management Act 1994

Victoria: Standing Directions of the Minister of Finance under the Financial Management Act 1994

AS/NZS ISO 27001, Information Security Standards, Standards Australia.

AS/NZS ISO 27002, Information Technology - Security Techniques, Code of Practice for information security information controls

11 Records

Records will be maintained in accordance with the requirements of Box Hill Institute's Records Management Policy and Procedures.

Where the privacy of individuals may otherwise be compromised, records will be maintained as confidential.

12 Review

This policy must be reviewed no later than three (3) years from the date of CEO endorsement. The policy will remain in force until such time as it has been reviewed and re-approved or rescinded. The policy may be withdrawn or amended as part of continuous improvement prior to the scheduled review date.

13 Responsibilities

14 Approval Body

The CEO is the approval body.

Owner	Author
Chief Operation Officer	Manager – Technology Solutions