MOBILE DEVICES POLICY – Version 2

Authorised by: CEO

Document: Mobile Devices Policy

Document No.: ITS-POL-003

Process Area: IT Services

1 Document Control

Version	Date	Amended by	Changes Made
0.1	20/01/2017	Information Technology Director	Initial document
0.2	29/03/2017	Senior Manager, Technology Solutions	Incorporate TS Team Feedback
1.0	14/04/2017	Senior Manager, Technology Solutions	Executive feedback and approval
1.2	17/05/2019	Academic Quality Assurance Officer	Minor administrative changes to remove reference to BHIG & CAE
2.0	1/10/2021	Chief Information Officer	Major review and update to simplify and improve clarity within Policy between BHI owned and personally owned devices. Includes input from IT and non-IT stakeholders

2 Purpose

This Mobile Devices Policy details the expectations and requirements for employees (including casuals), students, contractors and third parties for the use of mobile devices to access information stored on, or within BHI's network and computer systems (including services hosted via third party arrangements).

3 Scope

This policy is applicable to all BHI employees (including casuals), students, contractors, third parties and any other personnel who use mobile devices to access BHI information and/or systems. Mobile devices includes smartphones, tablets, smartwatches, laptops, tablet PCs or similar, both BHI supplied as well as personally owned "Bring your own devices" (BYOD).

4 Policy Statement

4.1 BHI Owned Devices and Services

BHI endorses the use of mobile devices in support of greater work flexibility and productivity. To ensure the security of BHI information and systems is maintained, as well as undertaking effective operational management of mobile devices, BHI has defined a set of requirements that will apply to all users of mobile devices. These are:

i. Access to BHI information services and systems via mobile devices will be restricted to authorised individuals only with access approved and granted by BHI.

ii. Access requests will be submitted via IT Services and supported by applicable line manager or business area authorisation.

iii. Use of mobile devices must comply with this *Mobile Devices Policy*, the *Acceptable Use of ICT Resources Policy* and BHI's *Staff Code of Conduct*.

iv. Mobile device standards and specifications will be defined by IT Services with input from applicable stakeholders within BHI.

v. The purchasing of BHI funded mobile devices must be via IT Services with pre-requisite approvals to purchase as defined within the *ICT Equipment Allocation Policy*.

vi. Budget for the acquisition and operating costs for different mobile device types will be undertaken as defined within the *ICT Equipment Allocation Policy*.

vii. BHI will periodically reassess which information systems and services will be made accessible via mobile devices.

viii. All mobile devices must be kept up to date with operating system and security patches, and applicable security software in a timely manner. BHI reserves the right to restrict devices from accessing BHI information as this statement refers to and systems which are significantly out of date and/or deemed vulnerable to security exploitations.

ix. Unsupported or customised versions of mobile operating systems (IOS, Android, Windows), including "jailbroken" mobile operating systems are not allowed to access BHI's networks and systems.

x. Access control on mobile devices will be compliant with BHI's *Access Management Policy*.

xi. Users must take reasonable steps to protect all mobile devices from damage or theft. For example, user should maintain line of sight with the device at all times in public spaces. Use appropriate protective casing.

xii. Costs to replace or repair a mobile device will be covered by the staff member if proven to be caused by deliberate or negligent behaviour. Examples of what may constitute negligent behaviour include users repeatedly losing or damaging their mobile device or using a device in a situation that it was not designed for (eg. swimming).

xiii. All lost, stolen or compromised BHI mobile devices must be reported immediately to the IT Service Desk with subsequent steps to be undertaken as defined within the *ICT Equipment Allocation Policy.*

xiv. In the event of a security breach, BHI may revoke employee and/or mobile device access without notice.

xv. All BHI owned mobile devices must be maintained in the IT asset register along with assignee details.

xvi. Users should not alter or attempt to alter BHI stipulated device settings and configurations.

xvii. Users should not rely on the mobile device as the only repository for BHI information/data and ensure all data is backed up or available via BHI network or system.

xviii. It is the responsibility of each user to secure and backup information stored on mobile devices in their possession. BHI takes no responsibility for any loss of data on devices including personal data (such as photos, music, videos or emails).

xix. BHI information must not be backed up to non-BHI devices or services without prior authorisation by IT Services. This includes backing up to personal computers and non-BHI provided cloud storage services. NB: Sharing or transfer of information to third parties is permissible where the security of the information can be reasonably assured and is

operationally required to do so. Third parties include (but are not limited to) DET, commercially contracted customers and suppliers, regulators, sector peers and partners.

xx. Care must be taken not to expose BHI information stored on or available via mobile devices to unauthorised parties, including friends, family members or other third parties.

xxi. Excess voice and data usage will be monitored on all BHI owned mobile data services. BHI reserves the right to seek reimbursement for excess usage costs caused by non-work related use.

xxii. Authorisation must be granted by the CEO, with approval submitted to IT Services to activate International roaming prior to the staff member departing overseas. BHI reserves the right to seek reimbursement for all costs attributed to personal use including all global roaming voice and data costs.

xxiii. Access to BHI information from mobile devices should be protected using secure encrypted methods such as https and VPN. NB: This is particularly important in potentially insecure environments such as the use of public Wi-Fi service providers.

xxiv. At the cessation of employment, Mobile devices (along with all other assigned devices) must be returned to IT Services to be reconfigured and re-deployment.

xxv. BHI Mobile devices are for the use of BHI employees only to conduct activities related to BHI employment conditions and are not to be used by friends or family members or any other non-BHI personnel.

4.2 BHI Mobile Device Management

For centralised management of mobile devices, BHI will deploy Mobile Device Management (MDM) software that is compatible with different device types and operating systems. MDM software capabilities allows BHI to better protect the security of the device and the information stored on them in a consistent and standardised way.

The following outlines what BHI will and won't use the MDM software for.

BHI will:

i. Manage all smartphones and non-Windows based tablet devices with access to BHI information using BHI's Mobile Device Management (MDM) software.

ii. Enforce mobile device configuration using Mobile Device Management (MDM) for the purposes of maintaining the security and operability of the device with BHI systems.

iii. Enforce access control on MDM managed devices to prevent unauthorised access to BHI information. This includes the deployment of minimum PIN and password rules to control access.

iv. Deploy and enforce system updates for MDM managed devices. BHI reserves the right to prohibit devices that have fallen unreasonably behind available operating system or firmware versions to connect to BHI's networks and systems.

v. Collect and store relevant device and system information, including operating system/firmware version information only for the purposes of device management, security and operability.

vi. Use MDM generated geo-location tracking information for the sole purpose of locating lost or stolen devices and at the request of the device assignee or owner.

vii. Prohibit the use of non-BHI provided cloud based backup functionality on smartphones and non-Windows tablet devices to back up BHI information.

viii. If the device is lost or stolen, reserve the right to initiate a remote device wipe (either partially or fully) to remove all BHI information off the device.

ix. Reserve the right to enforce deployment of mobile device endpoint security on MDM managed devices.

BHI will not:

i. Collect and store device information for reasons other than those stated within this Policy.

ii. Access, collect or store geo-location tracking information for the purposes of monitoring user location and movements outside of those stated above.

iii. Access, collect or store details of non-BHI installed applications or any other non-BHI related content that is stored on a personally owned mobile device.

iv. Initiate a remote device wipe that will delete personal information on a personally owned mobile device, without the device owners consent.

4.3 BHI Windows Based Mobile Devices

Laptops and Tablets are considered a mobile device and operate using the Microsoft Windows operating system, with access controlled by Microsoft Active Directory. BHI has deployed Microsoft System Centre Configuration Manager (SCCM) and Microsoft InTune to manage all Windows devices. The following requirements are specific to these devices.

i. System updates will be enforced through SCCM or InTune in accordance with BHI's device patching cycles.

ii. Device configuration (including security) will be enforced via Microsoft Active Directory and supporting tools and software.

iii. Devices must be connected regularly to BHI's network to receive the latest updates and configuration. If critical or urgent updates are required, users may be requested to connect to BHI's network as soon as practicable to ensure device remains secure.

4.4 Personally Owned Devices – Employees, Casuals & Contractors

The following applies to all Employees, Casuals and Contractors who choose to use personally owned mobile devices to access BHI's network, systems and services:

i. Unless an exemption is approved by the Chief Information Officer, all mobile devices will have MDM software installed.

ii. To connect a personally owned mobile device to BHI's network, systems and services, a user must submit a service request to the IT Service Desk and be required to sign an agreement allowing BHI to install MDM software (unless exemption granted) and undertake management and security control activities as stated in Section 4.2 above.

iii. BHI will only provide support, advice or consulting services for personal mobile devices outside of issues related to the access of corporate applications on a best efforts basis only.

iv. BHI takes no responsibility for any damage to, or loss of personal devices including any information stored on these devices.

v. BHI will not delete non-BHI information stored on an MDM managed device without the consent of the device owner.

vi. All device costs associated with the acquisition, use or replacement of a personally owned device will remain the sole responsibility of the device owner.

vii. By agreement with the Business Area/Department Manager or Executive Director, voice or data charges attributed to business use may be reimbursed by BHI.

viii. Other than via an approved remote access method outlined within BHI's Remote Access Policy, personally owned Windows or non-Windows laptops and tablets will not be permitted to connect to BHI's Active Directory Services without prior approval from the Chief Information Officer.

ix. Approval for users to connect a personally owned mobile devices to the BHI's network, systems and services will be subject to device meeting minimum security standards set by BHI.

x. To protect BHI and user data/information, mobile device applications used should only be installed from a legitimate and trusted source. Examples of legitimate application sources are Apple iTunes/App Store and Google Play.

4.5 Personally Owned Devices – Students & Visitors

The following applies to Students and Visitors who use personally owned mobile devices to access BHI's network, systems and services:

i. Student and Visitor access to the BHI corporate network, systems and services is not permissible.

ii. Students will only be permitted to access the Student network and the systems and services required to undertake their studies and only for the duration of those studies.

iii. Vistitors isitors are permitted to access the Internet via BHI's Guest/Public Wi-Fi Service by accepting BHI's Terms and Conditions at the time of connection.

5 Occupational Health and Safety and Legislation

i. All users are responsible for ensuring that their use of mobile devices is safe and in accordance with Occupational Health & Safety Policies and guidelines.

ii. All users must ensure compliance with legislation governing the use of mobile devices whilst driving.

iii. BHI is not responsible for any fines incurred by users, or accidents involving users where these result from the improper use of mobile devices.

6 Code of Conduct

The Box Hill Institute has clear codes of conduct for staff and students and will not tolerate behaviour that does not meet our standards..

7 Definitions

Term	Definition
BHI	Box Hill Institute
Cloud Storage Services	Storage services provided by external vendors and hosted offsite within datacentres not belonging to BHI

Term	Definition
Contractors	All personnel not directly employed by BHI on a permanent, part-time or casual basis
Corporate Network	BHI Network restricted to BHI Employees
Employees	Includes all BHI employees irrespective of employment type
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) used for secure communication normally accessed via a Web Browser
Jailbroken	Common names for “cracked” or modified version of mobile operating systems, often allowing illegal access to applications and functionality not provided in official and supported releases from Google and Apple.
MDM (Mobile Device Management)	Software used for the management of mobile devices running Apple IOS or Android operating systems (and others as required)
Mobile Device	Portable computing devices such as Smartphones, Smart Watches, Laptops, Tablets or similar devices
Mobile Service	A company that offers mobile communication services to users of mobile devices such as smartphones and tablet PCs.
PIN	Personal Identifiable Number used for access control including on mobile devices.
Public Network	BHI Network accessible via Wi-Fi to enable access to Internet without BHI authorisation
Student Network	BHI Network made available to all student and public guests for the distribution of BHI Learning Materials
Third Parties	All organisations and their staff who are not directly employed by the BHI but who provide services to BHI.
Users	An all-encompassing term covering anyone using or interacting with an ICT product or service
VPN (Virtual Private Network)	A Virtual Private Network is an encrypted network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorised people from eavesdropping on the traffic and allows the user to conduct work remotely

8 Related Policies and Procedures

Staff and Student Code of Conducts

Acceptable Use of ICT Resources Policy

Remote Access Policy

Access Management Policy

Privay Policy

Copyright Policy

9 Related Operating Guidelines

N/A

10 Related Forms

N/A

11 Related Legislation and Regulations

11.1 Box Hill Institute

N/AExternal

Related Legislation and Registration

SEC POL 01 Information Security Management Policy, Victorian Government CIO BHI, 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

12 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 kept secure and confidential.

13 Review

This policy must be reviewed no later than three 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.

14 Responsibilities

The **Executive Director, Strategy & Corporate Services** has overall accountability for the implementation of and compliance with this Policy.

The **Chief Information Officer (CIO)** is responsible for overseeing the implementation and

effectiveness of controls (including technology and procedures) to ensure the Policy is implemented and managed.

IT Services Department is responsible for the management of day-to-day activities and processes to support the implementation and compliance with this Policy

15 Policy Owner

The Executive Director, Strategy and Corporate Services is the owner of this policy.

Executive Director Signature	Date Endorsed	Name/Title
	12/11/21	Laura MacPherson ED Strategy and Corporate Services

Author	Name
Chief Information Officer	Haydon Sampson

16 Approval Body

The CEO is the approval body.

Signature	Date	Name/Title
	11 / 11 / 2021	Vivienne King CEO