FAQ & Help Guide
BYOD – Self Managed Service

This guide is designed to assist you by answering frequently asked questions and outlining known limitations of the service. Please select a section or question below.

Contents
What services does BYOD give me access to?.................................................................3
Which devices can I use for BYOD?.............................................................................3
How many devices can I connect?..................................................................................3
Does BYOD include Wi-Fi access?................................................................................3
Do I need a passcode on my device?.............................................................................3
Who pays for calls and data?.......................................................................................3
Who do I go to for support if I have issues?.................................................................3
How do I request access to the service via OPS?.........................................................4
Who do I select as my approving supervisor?..............................................................4
I’ve completed the OPS process, but haven’t heard any further. What now?.................4
Who do I go to for support if I have issues?.................................................................4
Adding a new device via the user Portal....................................................................5
How do I generate a PIN via the user portal?...............................................................5
I cannot access the portal, I am not authorised, or the page is not found. ....................5
The portal is not accepting my login details..................................................................5
Do I need to enter my mobile number? .......................................................................5
Who do I go to for support if I have issues?.................................................................5
Activating your mobile device....................................................................................6
How do I activate my device?.......................................................................................6
How much data does the activation use?.....................................................................6
The Mobile@Work client is rejecting my activation PIN.............................................6
The Mobile@Work application says my device is not supported...............................6
Why does the Mobile@Work app require device permissions?....................................6
Why do I need to set a passcode on my device?.........................................................6
I’ve completed the process, but there’s no mail.........................................................6
Who do I go to for support if I have issues?.................................................................6
Using the new BYOD Service – Android Devices......................................................8
Why are emails in a separate app and not my native email app?.................................8
The Docs@Work application won’t launch.................................................................8
How do I attach files to emails?..................................................................................8
Can I add a secondary / additional mailbox to my Android device?.........................8
Can I open email which has been archived?..............................................................8
How do I connect to Staff Wi-Fi?................................................................................8
Why does my device lock so quickly?..........................................................................8
My device is warm and battery draining – Why?......................................................9
Android Activation Issue: failed profile.....................................................................9
Issues removing Mobile@work on Android...............................................................9
Issues resetting device passcode...........................................................................................................9
Who do I go to for support if I have issues?...........................................................................................9

**Using the new BYOD Service – iOS Devices** ..................................................................................10

What's the “VPN” logo in the corner of my screen? ...............................................................................10
The ‘Tunnel’ app never downloaded......................................................................................................10
QHEPS seems to take a long time to load on first attempt, why? ..........................................................10
Can I add a secondary / additional mailbox to my Apple device? ......................................................10
Can I open email which has been archived? ............................................................................................10
How do I connect to Staff Wi-Fi? .............................................................................................................10
Why does my device lock so quickly? .........................................................................................................10
My device is warm and battery draining – Why? .....................................................................................10
Who do I go to for support if I have issues? .............................................................................................11

**Further Information** ..........................................................................................................................12

What do I do if my device is lost or stolen? ............................................................................................12
How do I connect a second device? ..........................................................................................................12
How do I remove a single device from the service? ...............................................................................12
What do I do if I upgrade my device? ......................................................................................................12
I no longer want to be a part of the BYOD service ..............................................................................12
How do I get help if I need it? ....................................................................................................................12
I require a higher level of support. What are my options? .....................................................................12
An important note about Privacy & Security............................................................................................13
Getting Started & Prerequisites

What services does BYOD give me access to?
The BYOD – Self Managed Service gives you access to Queensland Health Mail, Contacts, Calendar and selected Intranet services (eg. QHEPS).

Which devices can I use for BYOD?
The service works with iOS (Apple) and Android (Google) smartphones and tablets running recent versions of operating system software, being iOS 8 and above, or Android 4.3 and above. Unfortunately, existing BlackBerry 10 devices are not able to be used with the new system.

How many devices can I connect?
You may connect up to 3 devices simultaneously on the BYOD – Self Managed Service.

Does BYOD include Wi-Fi access?
It does depending on where you are. Staff Wi-Fi is being rolled out across the state. To see if Staff Wi-Fi is available in your area, click here.

If a location near you isn't listed yet don't fret, the BYOD project is always expanding and looking to include more sites shortly. Keep an eye on the BYOD QHEPS page and the BYOD Yammer page for updates to new sites.

Do I need a passcode on my device?
To ensure security, a passcode is enforced on all BYOD devices. The passcode must be 6 digits and not contain repeating or simple characters (eg. 111111 or 123456). You may still choose to set up fingerprint unlock in conjunction with a 6 digit backup password. You may also use a pattern lock with 6 or more touch points.

Who pays for calls and data?
For personal devices, all calls and data usage are the responsibility of the user.

Who do I go to for support if I have issues?
If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You'll also find a great selection of guides and FAQ documents to assist you.

The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the Fully Managed Corporate Service offered by the Smart Device Team within eHealth.
Requesting the service via OPS

How do I request access to the service via OPS?
Please refer to the document located here.

Who do I select as my approving supervisor?
Your supervisor is your immediate superior within the organisation. You may wish to advise your supervisor that you are applying for the service.

I’ve completed the OPS process, but haven’t heard any further. What now?
Your supervisor must approve your application before the process can continue. You may wish to follow up with your supervisor to expedite this step.

Who do I go to for support if I have issues?
If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You'll also find a great selection of guides and FAQ documents to assist you.

The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the Fully Managed Corporate Service offered by the Smart Device Team within eHealth.
Adding a new device via the user Portal

How do I generate a PIN via the user portal?
Please refer to the document located here.

I cannot access the portal, I am not authorised, or the page is not found.
The user portal (https://vsp.mdm.health.qld.gov.au) may present an error "HTTP Status 403 - Access is denied, you are unauthorized to access this page." when attempting to access from a non-QH PC/workstation. The portal will not provide any opportunity to log in, there is no prompt for username / password.
You can only access the portal from a Queensland Health computer. Ensure you are using a QH PC and are connected to the QH network. The portal is not accessible from a BYOD mobile device. Please attempt to access the portal from a QH PC.

The portal is not accepting my login details. It says that I am not authorised.
The error message that will be presented after attempting to login is “You are unauthorized to access this page.”
You cannot log into the portal until you have applied via OPS, been approved by your supervisor, and waited 30 minutes after receiving a confirmation email from OPS.
If you are certain that you have applied and have been approved to use the service, wait 15 minutes and retry, ensuring that your username and password are correct.

Do I need to enter my mobile number?
As per the work instruction, you do not have to provide your mobile number when requesting a PIN. Your PIN will be emailed to you on your Queensland Health address.

Who do I go to for support if I have issue?
If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You'll also find a great selection of guides and FAQ documents to assist you.
The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the Fully Managed Corporate Service offered by the Smart Device Team within eHealth.
Activating your mobile device

How do I activate my device?

Activation instructions will be sent to your Queensland Health email address once you generate a device activation pin via the Self Support Portal. Refer to the section in this document titled "How do I generate a PIN via the user portal?" for instructions.

How much data does the activation use?

The Mobile@Work application is only approximately 10mb, however during the activation your email account can pull down a large volume of emails. It is advised that if you have limited mobile data you connect to a personal wi-fi network prior to activation to reduce your mobile data usage and not incur any large usage bills. Don’t forget that if you’re at one of the sites where Staff Wi-Fi is available you should also have access to Guest Wi-Fi. You’re able to use this Guest Wi-Fi to perform the activation and get yourself setup on BYOD.

The Mobile@Work client is rejecting my activation PIN.

If you are presented with a ‘Request Forbidden’, or ‘Invalid Credentials’ message, please wait 15 minutes, login to the portal from a QH computer (http://vsp.mdm.health.qld.gov.au), ‘retire’ the device you were attempting to activate, and then re-request an activation PIN. Follow this guide if you prefer step-by-step guidance to remove the pending device, then follow the steps for generating an activation PIN again.

If you have tried all of the above steps and are still receiving an error please contact the InfoService Centre on 1800 198 175 and ask them to confirm your Novell account is unlocked.

The Mobile@Work application says my device is not supported.

Only Android 4.3+ and iOS 8.0+ devices are supported at this time. If possible, try to update the software on your device.

Why does the Mobile@Work app require device permissions?

In order to function and enforce basic security (eg. a passcode), the client requires access to many permissions on your device. Be assured that your personal information remains personal, and the service has no ability to access your personal text messages, photos or voicemail.

Why do I need to set a passcode on my device?

To ensure security, a passcode is enforced on all BYOD devices. The passcode must be 6 digits and not contain repeating or simple characters (eg. 111111 or 123456). You may still choose to set up fingerprint unlock in conjunction with a 6 digit backup password. You may also use a pattern lock with 6 or more touch points.

I’ve completed the process, but there’s no mail.

After completing the activation process, please wait at least 5 minutes for the device to connect to the server before launching the mail client. On iOS, you’re launching the native ‘Mail’ app. On Android, you’re looking for the green ‘Mail’ application which has been added to your device.
Who do I go to for support if I have issues?

If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for "BYOD") on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You’ll also find a great selection of guides and FAQ documents to assist you.

The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the Fully Managed Corporate Service offered by the Smart Device Team within eHealth.
Using the new BYOD Service – Android Devices.

Why are emails in a separate app and not my native email app?
Due to the large number of Android flavours and versions, we’ve had to use a containerised application approach for Android to ensure a consistent experience across devices. For many Android devices, pushing corporate email to the native email application is simply not possible. In future, solutions such as Google’s Android for Work mechanism may be used; however this functionality will only be available on newer devices once implemented.

The Docs@Work application won’t launch.
An issue has been identified on some devices and Android versions where the Docs@Work application will not load. If you are encountering this, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au).

How do I attach files to emails?
Some limitations exist with the current version of the Android container. To attach a photo to an email, just tap ‘attach’ within a compose email screen and select an image from your personal gallery. To attach a document from Docs@Work, you’ll need to launch the Docs@Work application first, open the attachment, and share via email. Currently you cannot attach files from the personal file manager to a corporate email.

Can I add a secondary / additional mailbox to my Android device?
At this point you aren’t able to add a secondary mailbox to your Android device. It is however being looked into for the future so keep an eye on the BYOD QHEPS page and the BYOD Yammer page for any updates.

Can I open email which has been archived?
Due to the way the Enterprise Vault archiving solution works, emails may be unavailable to open once archiving has occurred. You can still access archived emails from a Queensland Health computer.

How do I connect to Staff Wi-Fi?
Once you have enrolled and are at a site that supports Staff Wi-Fi all you should need to do is turn on your Wi-Fi. Your device should automatically connect, however if it doesn’t open up your Wi-Fi settings and search for ‘QH-BYOD’. If you can see the network tap it and your device should connect, if you can’t see the network you may not be in range of an access point.

Why does my device lock so quickly?
For security reasons, the device is required to lock after 5 minutes of inactivity. This prevents situations of data loss if your device is left unattended.
My device is warm and battery draining – Why?

During the first 48 hours after activating to the BYOD service, your device is busy downloading emails, contacts, calendars as well as indexing all this information. It’s not unusual for higher rates of battery drain to occur, or for the device to warm while processing information.

Further, after the initial sync period, your device will still be receiving larger than normal amounts of emails which will result in slightly lower battery life. This is expected behaviour when adding a new inbox to your device.

Android Activation Issue: failed profile

When attempting to activate on an Android device, you may receive an error stating “Your company has set up a work profile” or a failure referring to “Knox”.

If this is the case, check if there is an application called “My Knox” and remove it from the device. You may have to use the Google Play Store app to locate and remove “My Knox”.

Once My Knox is removed, re-try activation.

Issues removing Mobile@work on Android

If you experience issues removing the Mobile@Work app on an Android – you may have to first turn off Device Administrator.

First, you need to disable the device administrator for the app. If you go into settings, you should find a "lock screen and security" menu (or similar). Then "Other Settings" and look for "Device Administrators". If there’s a Mobile@Work entry there, see if it allows you to disable/turn off the device administrator. Now see if the device permits you to delete (uninstall) the Mobile@Work app.

Once the app is uninstalled, you may then re-install a fresh copy of the app and re-activate.

Issues resetting device passcode

With Androids release of OS 7, you will no longer be able to reset your device passcode from the customer portal. You will need to reset your device back to factory settings to remove the device passcode.

Who do I go to for support if I have issues?

If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You’ll also find a great selection of guides and FAQ documents to assist you.
Using the new BYOD Service – iOS Devices.

What’s the “VPN” logo in the corner of my screen?
The new BYOD service uses VPN on-demand technology to connect to certain internal resources including QHEPS. This logo simply means that your device is, or has connected to work infrastructure – a completely normal process while processing work emails or accessing intranet sites.

The ‘Tunnel’ app never downloaded.
If the Tunnel app does not appear or if installation of Tunnel was unintentionally cancelled, you may re-involve the installation by launching the Apps@Work application and tapping ‘request’ on the tunnel icon under ‘featured apps’.

QHEPS seems to take a long time to load on first attempt, why?
When first attempting to access QHEPS on your device, a VPN on-demand session must be established. This takes a few moments, but once it’s connected, you should find faster response.

Can I add a secondary / additional mailbox to my Apple device?
Yes, assuming you have full access to a shared / secondary mailbox, you can request access to add this mailbox to your Apple device (Secondary mailboxes on Android devices are not currently supported). To request access to a secondary mailbox on your Apple device, follow the work instruction found here: Adding a secondary mailbox. You may only have one secondary mailbox linked to your account at any given time.

Can I open email which has been archived?
Due to the way the Enterprise Vault archiving solution works, emails may be unavailable to open once archiving has occurred. You can still access archived emails from a Queensland Health computer.

How do I connect to Staff Wi-Fi?
Once you have enrolled and are at a site that supports Staff Wi-Fi all you should need to do is turn on your Wi-Fi. Your device should automatically connect, however if it doesn’t open up your Wi-Fi settings and search for ‘QH-BYOD’. If you can see the network tap it and your device should connect, if you can’t see the network you may not be in range of an access point.

Why does my device lock so quickly?
For security reasons, the device is required to lock after 5 minutes of inactivity. This prevents situations of data loss if your device is left unattended.

My device is warm and battery draining – Why?
During the first 48 hours after activating to the BYOD service, your device is busy downloading emails, contacts, calendars as well as indexing all this information. It’s not unusual for higher rates of battery drain to occur, or for the device to warm while processing information.
Further, after the initial sync period, your device will still be receiving larger than normal amounts of emails which will result in slightly lower battery life. This is expected behaviour when adding a new inbox to your device.

**Who do I go to for support if I have issues?**

If you need assistance or wish to provide assistance to others, refer to the [BYOD Peer Support Community](https://www.yammer.com/health.qld.gov.au) (or search for “BYOD”) on Yammer. The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You’ll also find a great selection of guides and FAQ documents to assist you.

The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the [Fully Managed Corporate Service](#) offered by the Smart Device Team within eHealth.
Further Information

What do I do if my device is lost or stolen?

If you have access to a Queensland Health PC, log into the user portal (https://vsp.mdm.health.qld.gov.au) with your QH username and password. You may then attempt to locate the device assuming it is still in contact with the server. The next step is to secure work data by retiring the device. Note: Once you retire the device, you can no longer locate the device, so ensure you attempt to locate first.

Should you not have access to a Queensland Health PC, or should you wish to erase your device, please contact the Smart Device Team on 1800 066 888 (option ##2). Please note this phone number is only to be used for lost or stolen devices, and no other support will be offered for devices connected to the BYOD – Self Managed service.

How do I connect a second device?

Refer to the steps for generating an activation PIN for the new device.

How do I remove a single device from the service?

If you have access to a Queensland Health PC, log into the user portal (https://vsp.mdm.health.qld.gov.au) with your QH username and password. You may then choose the device you wish to remove, and ‘Retire’ the device. Follow this guide if you prefer step-by-step guidance.

What do I do if I upgrade my device?

If you have access to a Queensland Health PC, log into the user portal (https://vsp.mdm.health.qld.gov.au) with your QH username and password. You may then choose your ‘old’ device, and ‘Retire’ the device. Follow this guide if you prefer step-by-step guidance to remove the device. Then follow the steps for generating an activation PIN for the new device.

I no longer want to be a part of the BYOD service.

First, follow this guide to retire each connection device, then follow the instructions found here to revoke all access to the BYOD service.

How do I get help if I need it?

If you need assistance or wish to provide assistance to others, refer to the BYOD Peer Support Community (or search for “BYOD”) on Yammer (https://www.yammer.com/health.qld.gov.au). The Peer Support Community is your forum to ask questions, share experiences and share your knowledge with others. You’ll also find a great selection of guides and FAQ documents to assist you.

I require a higher level of support. What are my options?

The BYOD Self Support Service is a free service and does not offer phone support. Should you find yourself in need of a premium supported service, you may wish to consider the Fully Managed Corporate Service offered by the Smart Device Team within eHealth.
An important note about Privacy & Security

We value your privacy and appreciate the importance of balancing security, usability and privacy of your data and device. Here’s a quick guide to privacy and security on your device:

Personal content remains personal.

We cannot view your personal email, iMessage, SMS, photos, videos or voicemail. We also cannot view personal contacts or calendar entries assuming the default contact and calendar are set to a personal (non-QH) address book or calendar.

When connecting your personal device to Queensland Health systems, Apple’s iOS operating system sometimes sets your work email, contacts and calendar as the default accounts.

This means that new contacts or appointments added to your device may synchronise with your Queensland Health account. To protect the personal information of your contacts, it is important that you change the default for your contacts and calendar to your personal email account, as follows:

Navigate to:
Settings > Contacts > Default Account (for Contacts)
and change the default to your personal account (if relevant)

then navigate to:
Settings > Calendar > Default Calendar (for Calendar)
and change the default to your personal account (if relevant)

What’s accessible by Queensland Health?

Some device details including model name, OS version and roaming status are accessible and used by the system to ensure you have the relevant versions of applications to connect to the system. Your device location (if enabled) is accessible in the event of a reported lost or stolen device. A list of installed apps and version numbers are collected and compared to a list of known malicious applications to ensure your device and data remains secure. Your Queensland Health emails, contacts and calendar (data synchronised with the ‘BYOD-iOS-Exchange’ account) remains auditable by Queensland Health and relevant authorities.

What actions can be taken on my device?

If your device is lost or stolen, you or Queensland Health may take security measures to protect your data. This includes the ability to clear the device passcode (in the event you forget your passcode), lock the device (in the event that your device is lost or misplaced), turn off roaming (if lost overseas), or erase the device (only in circumstances where a remote wipe is requested by you after the loss or theft of your device). Device erasure will also automatically occur if more than 8 consecutive failed attempts are made to unlock the device. To reduce the chances of accidental erasure, the device will pause (disable) for incrementally longer periods of time after each failed attempt.